

Accton

Making Partnership Work

CheetahSwitch Workgroup-3726M Management Guide



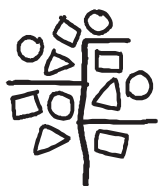


Making Partnership Work

Management Guide

CheetahSwitch Workgroup-3726M

*Intelligent Stackable Fast Ethernet Switch
with 24 10BASE-T / 100BASE-TX (RJ-45) Ports,
and Optional Media Expansion and Stack Modules*



Copyright © 2002 by Accton Technology Corporation. All rights reserved.

No part of this document may be copied or reproduced in any form or by any means without the prior written consent of Accton Technology Corporation.

Accton makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability, quality, or fitness for any particular purpose. The information in this document is subject to change without notice. Accton reserves the right to make revisions to this publication without obligation to notify any person or entity of any such changes.

On-line Registration

For quick warranty registration, log on our website at <http://register.acctontech.com> to register your Accton products.

Accton

International Headquarters

No. 1 Creation Road III,
Science-based Industrial Park
Hsinchu 300, Taiwan.
Phone: +886-3-5770-270
Fax: +886-3-5770-267
Internet: support@accton.com.tw

Asia Pacific Headquarters

1 Claymore Drive
#08-05/06 Orchard Towers (Rear Block)
Singapore 229594
Phone: +65 238 6556
Fax: +65 238 6466
Internet: www.acctontech.com

Europe Headquarters

Edificio Conata II,
Calle Fructuós Gelabert 6-8, 2^a, 4^a,
08970 - Sant Joan Despí,
Barcelona, Spain.
Phone: +34-93-477-4920
Fax: +34-93-477-3774

Accton is a trademark of Accton Technology Corporation. Other trademarks or brand names mentioned herein are trademarks or registered trademarks of their respective companies.

AC-ES3726M
E022002-R01
F2.4761 150000017100A

Accton Technology Corporation

Limited Warranty: Accton warrants all its products to be free of manufacturing defects in workmanship and materials, under normal use and service, for the applicable warranty term. All Accton products carry a standard 90-day limited warranty from the date of purchase from Accton or its Authorized Reseller. Accton may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from Accton or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the Accton web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" Accton product. A product is considered to be "Active" while it is listed on the current Accton price list. As new technologies emerge, older technologies become obsolete and Accton will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" Accton product. A list of discontinued products is attached with the firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to Accton pursuant to any warranty. Products returned to Accton should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. Accton is not responsible for these items if they are returned with the product.

Customers must contact Accton for a Return Material Authorization number prior to returning any product to Accton. Proof of purchase may be required. Any product returned to Accton without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. Customers are responsible for all shipping charges from their facility to Accton. Accton is responsible for return shipping charges from Accton to customer.

WARRANTIES EXCLUSIVE: IF AN ACCTON PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT ACCTON'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ACCTON NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. ACCTON SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE,

Limited Warranty

NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL ACCTON BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF ACCTON OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* Accton will provide warranty service for up to three years following discontinuance from the active Accton price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

Contents

Switch Management	1-1
Configuration Options	1-1
Required Connections	1-1
Console Port (Out-of-Band) Connections	1-1
In-Band Connections	1-2
Using the System Configuration Program	2-1
Login Screen	2-1
Console Configuration Navigation Keys and Buttons	2-3
Main Menu	2-4
System Information Menu	2-6
Displaying System Information	2-7
Displaying Switch Version Information	2-8
Management Setup Menu	2-9
Changing the Network Configuration	2-10
IP Configuration	2-11
IP Connectivity Test (Ping)	2-12
HTTP Configuration	2-13
Configuring the Serial Port	2-14
Assigning SNMP Parameters	2-15
Configuring Community Names	2-16
Configuring IP Trap Managers	2-17
Console Login Configuration	2-18
Downloading System Software	2-19
Using TFTP to Download Over the Network	2-19
Saving the System Configuration	2-20
Configuring the Switch	2-21
Configuring Port Parameters	2-22
Viewing the Current Port Configuration	2-23
Using the Spanning Tree Algorithm	2-24
Configuring Bridge STA	2-24
Configuring STA for Ports	2-26
Viewing the Current Spanning Tree Information	2-27
Displaying the Current Bridge STA	2-28
Displaying the Current STA for Ports	2-29
Using a Mirror Port for Analysis	2-30
Configuring Port Trunks	2-31
IGMP Multicast Filtering	2-34
Configuring IGMP	2-34
Configuring Broadcast Storm Control	2-35
Configuring Bridge MIB Extensions	2-36

Configuring Traffic Classes	2-37
Port Priority Configuration	2-38
802.1P Port Traffic Class Information	2-39
Configuring Virtual LANs	2-40
802.1Q VLAN Base Information	2-40
802.1Q VLAN Current Table Information	2-41
802.1Q VLAN Static Table Configuration	2-42
802.1Q VLAN Port Configuration	2-44
Port Security Configuration	2-45
Monitoring the Switch	2-46
Displaying Port Statistics	2-47
Displaying RMON Statistics	2-48
Displaying the Unicast Address Table	2-50
Displaying the IP Multicast Registration Table	2-51
Configuring Static Unicast Addresses	2-52
Resetting the System	2-53
Logging Off the System	2-53
Web-Based Management	3-1
Web-Based Configuration and Monitoring	3-1
Navigating the Web Browser Interface	3-2
Home Page	3-2
Configuration Options	3-3
Panel Display	3-3
Port State Display	3-4
Console Configuration	3-5
Main Menu	3-6
System Information	3-7
Switch Information	3-8
Main Board	3-8
Agent Module	3-8
Expansion Slot	3-9
IP Configuration	3-10
SNMP Configuration	3-11
SNMP Community	3-11
Trap Managers	3-12
Security Configuration	3-12
Change Password	3-12
Firmware Upgrade Options	3-13
Web Upload Management	3-13
TFTP Download Management	3-13
Configuration Save and Restore	3-14
Configuration Upload Management	3-14
Configuration Download Management	3-14
Address Table Configuration	3-15

Spanning Tree Algorithm (STA)	3-16
Spanning Tree Information	3-16
Spanning Tree	3-16
Ports	3-17
Spanning Tree Configuration	3-18
Switch	3-18
When the Switch Becomes Root	3-18
STA Port Configuration	3-19
Configuring Bridge MIB Extensions	3-20
Bridge Capability	3-20
Bridge Settings	3-21
Priority	3-22
Port Priority Configuration	3-22
Port Traffic Class Information	3-23
Configuring Virtual LANs	3-24
VLAN Basic Information	3-24
VLAN Current Table	3-25
VLAN Static List	3-26
VLAN Static Table	3-27
VLAN Static Membership by Port	3-29
VLAN Port Configuration	3-30
IGMP Multicast Filtering	3-31
Configuring IGMP	3-31
IP Multicast Registration Table	3-32
Port Menus	3-33
Port Information	3-33
Port Configuration	3-34
Expansion Port Information	3-35
Expansion Port Configuration	3-36
Port Broadcast Storm Protect Configuration	3-37
Port Security Configuration	3-38
Using a Port Mirror for Analysis	3-39
Port Trunk Configuration	3-40
Port Statistics	3-42
Etherlike Statistics	3-42
RMON Statistics	3-43
Advanced Topics	4-1
Layer 2 Switching	4-1
Spanning Tree Algorithm	4-1
Virtual LANs	4-2
Assigning Ports to VLANs	4-3
Port Overlapping	4-3
Automatic VLAN Registration (GVRP)	4-3
Forwarding Traffic with Unknown VLAN Tags	4-4

Contents

Forwarding Tagged/Untagged Frames	4-4
Connecting VLAN Groups	4-4
Multicast Filtering	4-5
IGMP Snooping	4-5
IGMP Protocol	4-5
Class-of-Service (CoS) Support	4-6
Port Trunks	4-6
SNMP Management Software	4-6
Remote Monitoring	4-7
Troubleshooting	A-1
Troubleshooting Chart	A-1
Upgrading Firmware via the Serial Port	A-2
Pin Assignments	B-1
Console Port Pin Assignments	B-1
DB-9 Port Pin Assignments	B-1
Console Port to 9-Pin DTE Port on PC	B-1
Console Port to 25-Pin DTE Port on PC	B-1
Glossary	
Index	

Chapter 1: Switch Management

Configuration Options

For advanced management capability, the Management Module provides a menu-driven system configuration program. This program can be accessed by a direct connection to the serial port on the rear panel (out-of-band), or by a Telnet connection over the network (in-band).

The management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent permits the CheetahSwitch Workgroup-3726M (AC-ES3726M) to be managed from any PC in the network using in-band management software.

The management agent also includes an embedded HTTP Web agent. This Web agent can be accessed using a standard Web browser from any computer attached to the network.

The system configuration program and the SNMP agent support management functions such as:

- Enable/disable any port
- Set the communication mode for any port
- Configure SNMP parameters
- Configure VLANs or multicast filtering
- Display system information or statistics
- Configure the switch to join a Spanning Tree
- Download system firmware
- Restart the system

Required Connections

Console Port (Out-of-Band) Connections

Attach a VT100 compatible terminal or a PC running a terminal emulation program to the serial port on the switch's rear panel. Use the null-modem cable provided with this package, or use a null modem connection that complies with the wiring assignments shown in Appendix B of this guide.

When attaching to a PC, set terminal emulation type to VT100, specify the port used by your PC (i.e., COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, and 19200 bps (for initial configuration). Also be sure to set flow control to "none." (Refer to "Configuring the Serial Port" on page 2-14 for a complete description of configuration options.)

Note: If the default settings for the management agent's serial port have been modified and you are having difficulty making a console connection, you can display or modify the current settings using a Web browser as described under "Console Configuration" on page 3-5.

In-Band Connections

Prior to accessing the Management Module via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using an out-of-band connection or the BOOTP protocol.

Note: By default BOOTP is disabled and the IP address is set to 10.1.0.1. To enable BOOTP, see "IP Configuration" on page 2-11.

After configuring the switch's IP parameters, you can access the on-board configuration program from anywhere within the attached network. The on-board configuration program can be accessed using Telnet from any computer attached to the network. The switch and stack can also be managed by any computer using a Web browser (Internet Explorer 4.0, or Netscape Navigator 4.0 or above), or from a network computer using network management software.

- Notes:**
1. Use the Network Configuration menu to specify the maximum number of simultaneous Telnet sessions that are supported by the system (up to four).
 2. The on-board program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Chapter 2: Using the System Configuration Program

Login Screen

Once a direct connection to the serial port or a Telnet connection is established, the login screen for the on-board configuration program appears as shown below.

```

          AAAAAA
        AAAAAAAAAA
        AAAAA  AAAAA
        AAAAA  AAAAA
      AAAAA  AAAAA  CCCCCC  CCCCCC  TTTTTTTTTT  OOOOOO  NN  NN
      AAAAA  AAAAA  CC  CC  CC  TT  OO  OO  NNN  NN
      AAAAA  AAAAA  CC  CC  CC  TT  OO  OO  NN  NN  NN
      AAAAA  AAAAA  CC  CC  CC  TT  OO  OO  NN  NN  NN
      AAAAA  AAAAA  CC  CC  CC  TT  OO  OO  NN  NN  NN
      AAAAA  AAAAA  CCCCCC  CCCCCC  TT  OOOOOO  NN  NN
      AAAAA  AAAAA  CCCCCC  CCCCCC  TT  OOOOOO  NN  NN

          CheetahSwitch Workgroup 3726M
      V2.4761 01-08-2002 (c) Copyright Accton Technology Corp.

          User name :
          Password :
```

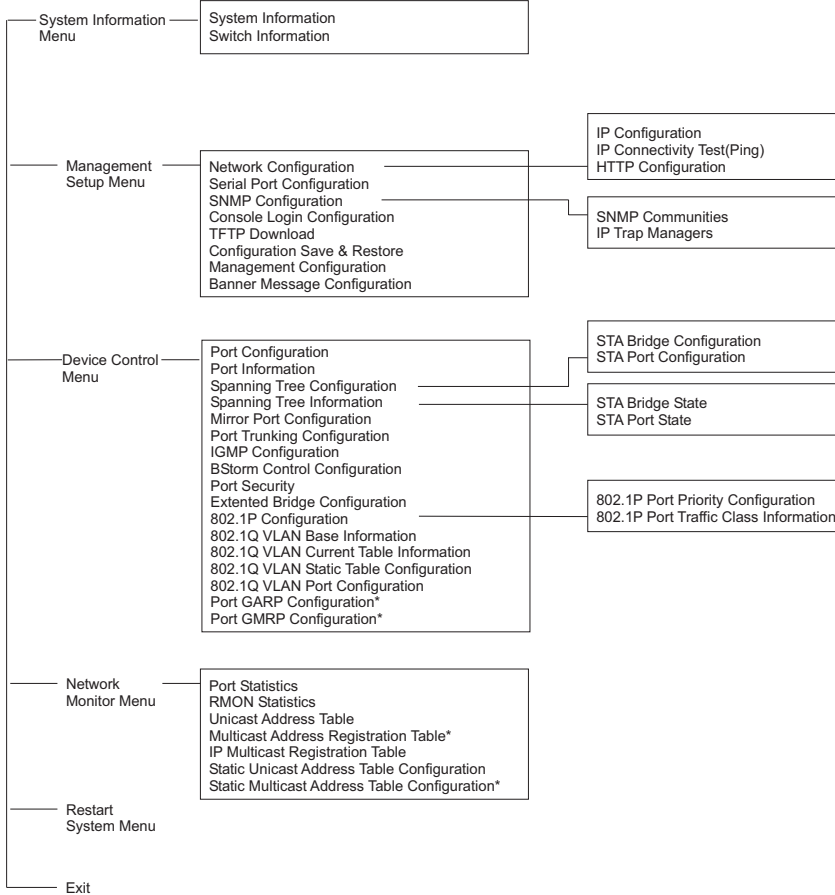
If this is your first time to log into the configuration program, then the default user names are "admin" and "guest," with no passwords. The administrator has Read/Write access to all configuration parameters and statistics. The guest has Read Only access to the management program.

You should define a new administrator password, record it and put it in a safe place. Select Console Login Configuration from the Management Setup Menu and enter a new password for the administrator. Note that passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

Note: Based on the default configuration, a user is allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

Using the System Configuration Program

After you enter the user name and password, you will have access to the system configuration program as illustrated by the following menu hierarchy:



* Not implemented in this firmware release.

Console Configuration Navigation Keys and Buttons

Menu items and configurable parameters in any screen can be selected by using <TAB> or the arrow keys. As you select each field, help information for the item is displayed in the highlighted line at the bottom of the screen. To change a setting, type in the parameter field or scroll through fixed options using the <Space> bar. If you make a configuration change on a screen, be sure to select the <APPLY> or <OK> button at the bottom of the screen to confirm the new setting.

The following table summarizes common screen configuration buttons.

Console Screen Configuration Buttons and Keys	
Button/Key	Action
<APPLY>	Sets specified values in the management agent.
<OK>	Sets specified values in the management agent and returns to the previous screen.
<CANCEL>	Cancels any modified screen settings (prior to pressing the <APPLY> button) and returns to the previous screen.
<PREV UNIT>	Selects the switch stack unit with the stack ID one less than the current unit.
<NEXT UNIT>	Selects the switch stack unit with the stack ID one more than the current unit.
<PREV PAGE>	Displays the previous page of data for the current screen.
<NEXT PAGE>	Displays the next page of data for the current screen.
<TAB> Key	Moves to the next selectable item in the screen.
<Arrow> Keys	Moves to the next selectable item (left/right/up/down) in the screen.
<Enter> Key	Selects the highlighted item in a screen.

Main Menu

With the system configuration program you can define system parameters, manage and control the switch, the connected stack and all its ports, or monitor network conditions. The figure below of the Main Menu and the following table briefly describe the selections available from this program.

Note: Options for the currently selected item are displayed in the highlighted area at the bottom of the interface screen.

```

                                Main Menu
                                =====

                                System Information Menu...

                                Management Setup Menu...

                                Device Control Menu...

                                Network Monitor Menu...

                                Restart System Menu...

                                Exit

                                Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
<i>System Information Menu</i>	
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, power status, and expansion modules used in the stack.
<i>Management Setup Menu</i>	
Network Configuration	Includes IP setup, Ping facility, HTTP (Web agent) setup, Telnet configuration, and MAC address.
Serial Port Configuration	Sets communication parameters for the serial port, including management mode, baud rate, console time-out, and screen data refresh interval.
SNMP Configuration	Activates traps; configures communities and trap managers.
Console Login Configuration	Sets user names and passwords for system access, as well as the invalid password threshold and lockout time.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Configuration Save & Restore	Saves the switch configuration to a file on a TFTP server. This file can be later downloaded to restore the configuration.

Menu	Description
<i>Device Control Menu</i>	
Port Configuration	Enables any port, enables/disables flow control, and sets communication mode to auto-negotiation, full duplex or half duplex.
Port Information	Displays operational status, including link state, flow control method, and duplex mode.
Spanning Tree Configuration	Enables Spanning Tree Algorithm; also sets parameters for hello time, maximum message age, switch priority, and forward delay; as well as port priority, path cost, and fast forwarding.
Spanning Tree Information	Displays full listing of parameters for the Spanning Tree Algorithm.
Mirror Port Configuration	Sets the source and target ports for mirroring.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
IGMP Configuration	Configures IGMP multicast filtering.
BStorm Control Configuration	Allows you to enable/disable broadcast storm control on a per-port basis and set the packet-per-second threshold.
Extended Bridge Configuration	Displays extended bridge capabilities provided by this switch.
802.1P Configuration	Configures default port priorities and queue assignments.
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported.
802.1Q VLAN Current Table Information	Displays VLAN groups and port members.
802.1Q VLAN Static Table Configuration	Configures VLAN groups via static assignments, including setting port members, or restricting ports from being dynamically added to a port by the GVRP* protocol.
802.1Q VLAN Port Configuration	Displays/configures port-specific VLAN settings, including PVID, ingress filtering, and GVRP*.
Port Security Configuration	Allows you to enable and configure port security for the switch.
Port GARP Configuration*	Configures settings used in multicast filtering.
Port GMRP Configuration*	Configures GMRP multicast filtering.
<i>Network Monitor Menu</i>	
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full listing for unicast addresses, as well as search and clear functions.
Multicast Address Registration Table*	Provides full listing for multicast addresses, as well as search and clear functions.
IP Multicast Registration Table	Displays all the multicast groups active on this switch, including multicast IP addresses and corresponding VLAN IDs.
Static Unicast Address Table Configuration	Used to manually configure host MAC addresses in the unicast table.
Static Multicast Address Table Configuration*	Used to manually configure host MAC addresses in the multicast table.
Restart System Menu	Restarts system with options to use POST, or to retain factory defaults, IP settings, or user authentication settings.
Exit	Exits the configuration program.

* Not implemented in this firmware release.

System Information Menu

Use the System information Menu to display a basic description of the switch, including contact information, and hardware/firmware versions.

```
System Information Menu
=====

System Information ...

Switch Information ...

                                <OK>

Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, power status, and expansion modules used in the stack.

Displaying System Information

Use the System Information screen to display descriptive information about the switch, or for quick system identification as shown in the following figure and table.

System Information
=====

System Description : CheetahSwitch Workgroup 3726M

System Object ID : 1.3.6.1.4.1.1.259.6.10.9

System Up Time : 459241 (0 day 1 hr 16 min 32 sec)

System Name : DEFAULT SYSTEM NAME

System Contact : DEFAULT SYSTEM CONTACT

System Location : DEFAULT SYSTEM LOCATION

<APPLY> <OK> <CANCEL>

Use <TAB> or arrow keys to move, other keys to make changes.

Parameter	Description
System Description	System hardware description.
System Object ID	MIB II object identifier for switch's network management subsystem.
System Up Time	Length of time the current management agent has been running. (Note that the first value is 1/100 seconds.)
Network Host Name*	Name assigned to the switch system.
System Contact*	Contact person for the system.
System Location*	Specifies the area or location where the system resides.

* Maximum string length is 255, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

Displaying Switch Version Information

Use the Switch Information screen to display hardware/firmware version numbers for the main board, as well as the power status.

```
Switch Information : Unit 1
=====

Main Board
Hardware Version      : V3.0
Firmware Version     : V1.29
Serial Number        : 00-00-04-00-00-00
Port Number          : 26
Internal Power Status : Active
Redundant Power Status : Inactive
Expansion Slot 1      : 2Port 100Base-FX (MMF)
Expansion Slot 2      : -----

Agent Module
Hardware Version      : V3.0 (850 CPU)
POST ROM Version      : V1.11
Firmware Version      : V2.4761
SNMP Agent            : Master

<OK>          <PREV UNIT>      <NEXT UNIT>
Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
<i>Main Board</i>	
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
Serial Number	The serial number of the main board.
Port Number	Number of ports on the switch (including modules).
Internal Power Status	Indicates if the primary power is active or inactive.
Redundant Power Status	Indicates if the redundant power is active or inactive.
Expansion Slot 1	Shows module type if inserted: (100BASE-FX, 1000BASE-SX or 1000BASE-LX).
Expansion Slot 2	Shows module type if inserted: (100BASE-FX, 1000BASE-SX, 1000BASE-LX or Stacking).
<i>Agent Module</i>	
Hardware Version	Hardware version of the agent module.
POST ROM Version	Power-On Self-Test version number.
Firmware Version	Firmware version of the agent module.
SNMP Agent	Shows if this module is Master or Backup Master.

Management Setup Menu

After initially logging onto the system, adjust the communication parameters for your console to ensure a reliable connection (Serial Port Configuration). Specify the IP addresses for the switch (Network Configuration / IP Configuration), and then set the Administrator and Guest passwords (Console Login Configuration). Remember to record them in a safe place. Also set the community string which controls access to the on-board SNMP agent via in-band management software (SNMP Configuration). The items provided by the Management Setup Menu are described in the following sections.

```

Management Setup Menu
=====

Network Configuration ...
Serial Port Configuration ...
SNMP Configuration ...
Console Login Configuration ...
TFTP Download ...
Configuration Save & Restore ...

                                <OK>
        Display or change network configuration.
        Use <TAB> or arrow keys to move. <Enter> to select.

```

Menu	Description
Network Configuration	Includes IP setup, Ping facility, HTTP (Web agent) setup, Telnet configuration, and MAC address.
Serial Port Configuration	Sets communication parameters for the serial port, including management mode, baud rate, console time-out, and screen data refresh interval.
SNMP Configuration	Activates traps; configures communities and trap managers.
Console Login Configuration	Sets user names and passwords for system access, as well as the invalid password threshold and lockout time.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Configuration Save & Restore	Saves the switch configuration to a file on a TFTP server. This file can be later downloaded to restore the configuration.

Changing the Network Configuration

Use the Network Configuration menu to set the bootup option, configure the switch's Internet Protocol (IP) parameters, enable the on-board Web agent, or to set the number of concurrent Telnet sessions allowed. The screen shown below is described in the following table.

```

                                Network Configuration
                                =====

                                IP Configuration ...

                                IP Connectivity Test(Ping) ...

                                HTTP Configuration ...

                                MAX Number of allowed Telnet sessions (1-4) : 4

                                Physical Address : 00-10-B5-FD-84-BB

                                <APPLY>           <OK>           <CANCEL>
                                Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
IP Configuration	Screen used to set the bootup option, or configure the switch's IP parameters.
IP Connectivity Test (Ping)	Screen used to test IP connectivity to a specified device.
HTTP Configuration	Screen used to enable the Web agent.
MAX Number of Allowed Telnet Sessions	The maximum number of Telnet sessions allowed to simultaneously access the agent module.
Physical Address	Physical address of the agent module.

IP Configuration

Use the IP Configuration screen to set the bootup option, or configure the switch's IP parameters. The screen shown below is described in the following table.

```

Network Configuration : IP Configuration
=====

Interface Type : Ethernet

IP Address   : 10.2.13.19

Subnet Mask  : 255.255.252.0

Gateway IP   :

IP State     : USER-CONFIG

<APPLY>      <OK>      <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Default	Description
Interface Type		Indicates that all interfaces on the switch are Ethernet. Management IP packets from the switch are encapsulated within an Ethernet frame for transmission over the Ethernet network.
IP Address	10.1.0.1	IP address of the stack you are managing. The system supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent module (or running management software) must have an IP address. Valid IP addresses consist of four decimal numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	255.255.0.0	Subnet mask of the switch you have selected. This mask identifies the host address bits used for routing to specific subnets.
Gateway IP		Gateway used to pass trap messages from the system's agent to the management station. Note that the gateway must be defined if the management station is located in a different IP segment. No gateway IP address is configured as the default.
IP State	USER-CONFIG	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BOOTP). Options include: USER-CONFIG - IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.) BOOTP Get IP - IP is enabled but will not function until a BOOTP reply has been received. BOOTP requests will be periodically broadcast by the switch in an effort to learn its IP address. (BOOTP values can include the IP address, default gateway, subnet mask, and TFTP server IP.)

IP Connectivity Test (Ping)

Use the IP Connectivity Test to see if another site on the Internet can be reached. The screen shown below is described in the following table.

Network Configuration : IP Connectivity Test (Ping)
=====

IP Address :

Test Times : 1Interval : 3

Success : 0Failure : 0

[Start]

<OK>

Use <TAB> or arrow keys to move, other keys to make changes.

Parameter	Description
IP Address	IP address of the site you want to ping.
Test Times	The number of ICMP echo requests to send to the specified site. Range: 1~1000
Interval	The interval (in seconds) between pinging the specified site. Range: 1~10 seconds
Success/Failure	The number of times the specified site has responded or not to pinging.

HTTP Configuration

Use the HTTP Configuration screen to enable/disable the on-board Web agent, and to specify the TCP port that will provide HTTP service. The screen shown below is described in the following table.

```

Network Configuration : HTTP Configuration
=====

HTTP Server           : ENABLED

HTTP Port Number      : 80


<APPLY>                <OK>                <CANCEL>

Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Description
HTTP Server	Enables/disables access to the on-board Web agent.
HTTP Port Number	Specifies the TCP port that will provide HTTP service. Range : 0~65535 Default : Port 80 (Telnet Port 23 is prohibited.)

Configuring the Serial Port

You can access the on-board configuration program by attaching a VT100 compatible device to the switch's serial port. (For more information on connecting to this port, see "Required Connections" on page 1-1.) The communication parameters for this port can be accessed from the Serial Port Configuration screen shown below and described in the following table.

Serial Port Configuration =====		
Management Mode	:	CONSOLE MODE
Baud rate	:	19200
Data bits	:	8
Stop bits	:	1
Parity	:	NONE
Time-Out (in minutes)	:	0
Auto Refresh (in seconds)	:	5
 <APPLY> <OK> <CANCEL> Use <TAB> or arrow keys to move, <Space> to scroll options.		

Parameter	Default	Description
Management Mode	Console Mode	Indicates that the console port settings are for direct console connection.
Baud rate	19200	The rate at which data is sent between devices. Options : 2400, 4800, 9600, 19200 and auto detection. Note that when auto detection is selected, you need to first press the Enter key once to set the data rate and initialize the connection.
Data bits	8 bits	Sets the data bits of the RS-232 port. Options : 7, 8
Stop bits	1 bit	Sets the stop bits of the RS-232 port. Options : 1, 2
Parity	None	Sets the parity of the RS-232 port. Options : none/odd/even
Time-Out	10 minutes	If no input is received from the attached device after this interval, the current session is automatically closed. Range : 0 - 100 minutes; where 0 indicates disabled
Auto Refresh	5 seconds	Sets the interval before a console session will auto refresh the console information, such as Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. Range : 0, or 5-255 seconds; where 0 indicates disabled

Assigning SNMP Parameters

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the on-board agent are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

```

                                SNMP Configuration
                                =====

                                Send Authentication Fail Traps : ENABLED

                                SNMP Communities ...

                                IP Trap Managers ...

                                <APPLY>                <OK>                <CANCEL>
                                Use <TAB> or arrow keys to move, <Space> to scroll options.
  
```

Parameter	Description
Send Authentication Fail Traps	Issue a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default is disabled.)
SNMP Communities	Assigns SNMP access based on specified strings.
IP Trap Managers	Specifies management stations that will receive authentication failure messages or other trap messages from the switch.

Configuring Community Names

The following figure and table describe how to configure the community strings authorized for management access. Up to 5 community names may be entered.

SNMP Configuration : SNMP Communities
=====

	Community Name	Access	Status
1.	public	READ/WRITE	ENABLED
2.			
3.			
4.			
5.			

<APPLY>

<OK>

<CANCEL>

Use <TAB> or arrow keys to move, other keys to make changes.

Parameter	Description
Community Name	A community entry authorized for management access. Default strings: public (read only), private (read/write) Maximum string length : 20 characters
Access	Management access is restricted to Read Only or Read/Write.
Status	Sets administrative status of entry to enabled or disabled.

Configuring IP Trap Managers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.

SNMP Configuration : IP Trap Managers

=====

IP Address	Community Name	Status
1.		
2.		
3.		
4.		
5.		

<APPLY>

<OK>

<CANCEL>

Use <TAB> or arrow keys to move, other keys to make changes.

Parameter	Description
IP Address	IP address of the trap manager.
Community Name	A community specified for trap management access.
Status	Sets administrative status of selected entry to enabled or disabled.

Console Login Configuration

Use the Management Setup: Console Login Configuration to restrict management access based on specified user names and passwords, or to set the invalid password threshold and time-out. There are only two user types defined, ADMIN (Administrator) and GUEST, but you can set up to five different user names and passwords. Only Administrators have write access for parameters governing the switch. You should therefore assign a user name and password to the default Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you cannot gain access to the System Configuration Program, contact Accton Technical Support for assistance.) The parameters shown on this screen are indicated in the following figure and table.

Console Login Configuration

=====

Password Threshold : 3

Lock-out Time (in minutes) : 0

User Type

User Name

Password

1. ADMIN admin

2. GUEST guest

3.

4.

5.

<APPLY>

<OK>

<CANCEL>

Use <TAB> or arrow keys to move, other keys to make changes.

Parameter	Default	Description
Password Threshold	3	Sets the password intrusion threshold which limits the number of failed logon attempts. Range : 0~65535
Lock-out Time	0	The time (in seconds) the management console will be disabled due to an excessive number of failed logon attempts. Range : 0~65535 (0 indicates disabled)
Admin*	name: admin password: null	Administrator has access privilege of Read/Write for all screens.
Guest*	name: guest password: null	Guest has access privilege of Read Only for all screens.

* Passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

Downloading System Software

Using TFTP to Download Over the Network

Use the TFTP Download menu to load software updates into the switch. The download file should be an CheetahSwitich Workgroup-3726M binary file from Accton; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

```

                                TFTP Download
                                =====
Download Server IP :

Agent Software Upgrade      : ENABLED
Download Filename           :
Download Mode                : PERMANENT

[Process TFTP Download]

Download status : Complete

<APPLY>          <OK>          <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.
  
```

Parameter	Description
Download Server IP	IP address of a TFTP server.
Agent Software Upgrade	Indicates that the switch is enabled for software upgrades.
Download Filename	The binary file to download.
Download Mode	Indicates a download to permanent flash ROM.

Note: You can also download firmware using the Web agent (page 3-13) or by a direct console connection after a restart (page A-2).

Saving the System Configuration

Use the Configuration Save & Restore menu to save the switch configuration settings to a file on a TFTP server. The file can be later downloaded to the switch to restore the switch's settings. The success of the operation depends on the accessibility of the TFTP server and the quality of the network connection. Parameters shown on this screen are indicated in the following figure and table.

```

                                Configuration Upload
                                =====

                                Upload Server IP      :
                                Upload Filename       :

                                [Process TFTP Upload]

                                Upload status    : Complete

                                Configuration Download
                                =====

                                Download Server IP   :
                                Download Filename    :

                                [Process TFTP Download]

                                Download status : Complete

                                <APPLY>             <OK>             <CANCEL>
                                Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
<i>Configuration Upload</i>	
Upload Server IP	IP address of a TFTP server.
Upload Filename	The name of the file to contain the switch configuration settings.
[Process TFTP Upload]	Issues a request to upload the configuration settings to the specified file on the TFTP server.
Upload Status	Indicates if an upload is "Complete" or "In Progress."
<i>Configuration Download</i>	
Download Server IP	IP address of a TFTP server.
Download Filename	The name of the file that contains the switch configuration settings you wish to restore.
[Process TFTP Download]	Issues a request to the TFTP server to download the specified file.
Download Status	Indicates if a download is "Complete" or "In Progress."

Configuring the Switch

The Device Control menu is used to control a broad range of functions, including port configuration, Spanning Tree, port mirroring, multicast filtering, and Virtual LANs. Each of the setup screens provided by these configuration menus are described in the following sections.

```

                                Device Control Menu
                                =====

Port Configuration ...           Extended Bridge Configuration ...
Port Information ...             802.1P Configuration ...
Spanning Tree Configuration ... 802.1Q VLAN Base Information ...
Spanning Tree Information ...    802.1Q VLAN Current Table Information ...
Mirror Port Configuration ...    802.1Q VLAN Static Table Configuration ...
Port Trunking Configuration ...  802.1Q VLAN Port Configuration ...
IGMP Configuration ...          Port Security Configuration ...
BStorm Control Configuration ... Port GARP Configuration ...
                                Port GMRP Configuration ...

                                <OK>
                                Use <TAB> or arrow keys to move. <Enter> to select.

```

Menu	Description
Port Configuration	Sets communication parameters for ports.
Port Information	Displays current port settings and port status.
Spanning Tree Configuration	Configures the switch and its ports to participate in a local Spanning Tree.
Spanning Tree Information	Displays the current Spanning Tree configuration for the switch and its ports.
Mirror Port Configuration	Sets the source and target ports for mirroring.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
IGMP Configuration	Configures IGMP multicast filtering.
BStorm Control Configuration	Allows you to enable/disable broadcast storm control on a per-port basis and set the packet-per-second threshold.
Extended Bridge Configuration	Displays/configures extended bridge capabilities provided by this switch.
802.1P Configuration	Configures default port priorities and queue assignments.
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported.
802.1Q VLAN Current Table Information	Displays VLAN groups and port members.
802.1Q VLAN Static Table Configuration	Configures VLAN groups via static assignments, including setting port members.
802.1Q VLAN Port Configuration	Displays/configures port-specific VLAN settings, including PVID and ingress filtering.
Port Security Configuration	Allows you to enable and configure port security for the switch.
Port GARP Configuration*	Configures generic attribute settings used in the spanning tree protocol, VLAN registration, multicast filtering.
Port GMRP Configuration*	Configures GMRP multicast filtering.

* Not implemented in this firmware release.

Configuring Port Parameters

Use the Port Configuration menus to set or display communication parameters for any port or module in the stack.

Port Configuration : Unit 1 Port 1 - 12 =====				
Flow Control on all ports : [Enable] [Disable]				
Port	Type	Admin	Flow Control	Speed and Duplex

1	10/100TX	ENABLED	DISABLED	AUTO
2	10/100TX	ENABLED	DISABLED	AUTO
3	10/100TX	ENABLED	DISABLED	AUTO
4	10/100TX	ENABLED	DISABLED	AUTO
5	10/100TX	ENABLED	DISABLED	AUTO
6	10/100TX	ENABLED	DISABLED	AUTO
7	10/100TX	ENABLED	DISABLED	AUTO
8	10/100TX	ENABLED	DISABLED	AUTO
9	10/100TX	ENABLED	DISABLED	AUTO
10	10/100TX	ENABLED	DISABLED	AUTO
11	10/100TX	ENABLED	DISABLED	AUTO
12	10/100TX	ENABLED	DISABLED	AUTO
<APPLY> <OK> <CANCEL> <PREV UNIT> <NEXT UNIT> <PREV PAGE> <NEXT PAGE> Use <TAB> or arrow keys to move. <Enter> to select				

Parameter	Default	Description																
Flow Control on all ports	Disabled	See “Flow Control” in this table.																
Type		Shows port type as: 10/100TX: 10BASE-T / 100BASE-TX 100FX: 100BASE-FX 1000SX: 1000BASE-SX 1000LX: 1000BASE-LX																
Admin	Enabled	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.																
Flow Control	Disabled	Used to enable or disable flow control. Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. IEEE 802.3x flow control is used for full duplex. Note that flow control should not be used if a port is connected to a hub.																
Speed and Duplex	Auto	Indicates current port speed and duplex mode. Note that autonegotiation is not available for the 100BASE-FX ports. <table><tr><th>Port Type</th><th>Speed</th><th>Duplex Mode</th><th>Flow Control</th></tr><tr><td>100BASE-FX</td><td>100M</td><td>full duplex</td><td>auto</td></tr><tr><td>1000BASE-SX</td><td>1000M</td><td>auto</td><td>auto</td></tr><tr><td>1000BASE-LX</td><td>1000M</td><td>auto</td><td>auto</td></tr></table> The 1000BASE-SX and 1000BASE-LX ports are fixed at 1000 Mbps but autonegotiate duplex mode. The 100BASE-FX module is fixed at the indicated speed and duplex mode. All media types can autonegotiate flow control.	Port Type	Speed	Duplex Mode	Flow Control	100BASE-FX	100M	full duplex	auto	1000BASE-SX	1000M	auto	auto	1000BASE-LX	1000M	auto	auto
Port Type	Speed	Duplex Mode	Flow Control															
100BASE-FX	100M	full duplex	auto															
1000BASE-SX	1000M	auto	auto															
1000BASE-LX	1000M	auto	auto															

Viewing the Current Port Configuration

The Port Information screen displays the port type, status, link state, and flow control in use, as well as the communication speed and duplex mode. To change any of the port settings, use the Port Configuration menu.

Port Information : Unit 1 Port 1 - 12					
=====					
Port	Type	Operational	Link	FlowControl InUse	Speed and Duplex InUse
1	10/100TX	YES	DOWN	-----	-----
2	10/100TX	YES	DOWN	-----	-----
3	10/100TX	YES	DOWN	-----	-----
4	10/100TX	YES	DOWN	-----	-----
5	10/100TX	YES	DOWN	-----	-----
6	10/100TX	YES	DOWN	-----	-----
7	10/100TX	YES	DOWN	-----	-----
8	10/100TX	YES	DOWN	-----	-----
9	10/100TX	YES	DOWN	-----	-----
10	10/100TX	YES	DOWN	-----	-----
11	10/100TX	YES	DOWN	-----	-----
12	10/100TX	YES	DOWN	-----	-----
<OK> <PREV UNIT> <NEXT UNIT> <PREV PAGE> <NEXT PAGE> Use <TAB> or arrow keys to move. <Enter> to select.					

Parameter	Description
Type	Shows port type as: 10/100TX: 10BASE-T / 100BASE-TX 100FX: 100BASE-FX 1000SX: 1000BASE-SX 1000LX: 1000BASE-LX
Operational	Shows if the port is functioning or not.
Link	Indicates if the port has a valid connection to an external device.
FlowControl InUse	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.
Speed and Duplex InUse	Displays the current port speed and duplex mode used. (Note that Auto-negotiation is not available for 100BASE-FX ports.)

Using the Spanning Tree Algorithm

The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network. For a more detailed description of how to use this algorithm, refer to “Spanning Tree Algorithm” on page 4-1.

```
< Spanning Tree Configuration Menu >

Spanning Tree Bridge Configuration

Spanning Tree Port Configuration

                                <Ok>

Use <TAB> or arrow keys to move. <Enter> to select.
```

Configuring Bridge STA

The following figure and table describe Bridge STA configuration.

```
Spanning Tree Configuration : STA Bridge Configuration
=====

Spanning Tree Protocol      : ENABLED

Priority                    : 32768

Hello Time (in seconds)    : 2

Max Age (in seconds)       : 20

Forward Delay (in seconds) : 15

                                <APPLY>                <OK>                <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Parameter	Default	Description
Spanning Tree Protocol	Enabled	Enable this parameter to participate in a STA compliant network.
Priority	32,768	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Enter a value from 0 - 65535. Remember that the lower the numeric value, the higher the priority.

Parameter	Default	Description
Hello Time	2	Time interval (in seconds) at which the root device transmits a configuration message. The minimum value is 1. The maximum value is the lower of 10 or $[(\text{Max. Message Age} / 2) - 1]$.
Max (Message) Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or $[2 \times (\text{Hello Time} + 1)]$. The maximum value is the lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$.
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The maximum value is 30. The minimum value is the higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$.

Configuring STA for Ports

The following figure and table describe port STA configuration.

Spanning Tree Port Configuration : Unit 1 Port 1 - 12				
=====				
Fast forwarding on all ports :			[Enable]	[Disable]
Port	Type	Priority	Cost	FastForwarding

1	10/100TX	128	19	ENABLED
2	10/100TX	128	19	ENABLED
3	10/100TX	128	19	ENABLED
4	10/100TX	128	19	ENABLED
5	10/100TX	128	19	ENABLED
6	10/100TX	128	19	ENABLED
7	10/100TX	128	19	ENABLED
8	10/100TX	128	19	ENABLED
9	10/100TX	128	19	ENABLED
10	10/100TX	128	19	ENABLED
11	10/100TX	128	19	ENABLED
12	10/100TX	128	19	ENABLED
 <APPLY> <OK> <CANCEL> <PREV UNIT> <NEXT UNIT> <PREV PAGE> <NEXT PAGE> Use <TAB> or arrow keys to move. <Enter> to select				

Parameter	Default	Description
Fast forwarding on all ports	Enabled	See "FastForwarding" in this table.
Type		Shows port type as: 10/100TX: 10BASE-T / 100BASE-TX 100FX: 100BASE-FX 1000SX: 1000BASE-SX 1000LX: 1000BASE-LX
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) The default and recommended range is: Ethernet: 100 (50~600) Fast Ethernet: 19 (10~60) Gigabit Ethernet: 4 (3~10) The full range is 0 - 65535.
Fast Forwarding*	Enabled	This parameter is used to enable/disable the Fast Spanning Tree mode for the selected port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding.

*Fast Forwarding enables end-node workstations and servers to overcome time-out problems when the Spanning Tree Algorithm is implemented in a network. Therefore, Fast Forwarding should only be enabled for ports connected to an end-node device.

Viewing the Current Spanning Tree Information

The Spanning Tree Information screen displays a summary of the STA information for the overall bridge or for a specific port. To make any changes to the parameters for the Spanning Tree, use the Spanning Tree Configuration menu.

< Spanning Tree Information Menu >

Spanning Tree Bridge State

Spanning Tree Port State

<Ok>

Use <TAB> or arrow keys to move. <Enter> to select.

Displaying the Current Bridge STA

The parameters shown in the following figure and table describe the current Bridge STA State.

Spanning Tree Information : STA Bridge Information	
=====	
Priority	: 32768
Hello Time (in seconds)	: 2
Max Age (in seconds)	: 20
Forward Delay (in seconds)	: 15
Hold Time (in seconds)	: 1
Designated Root	: 32768.0010B5FD84BB
Root Cost	: 0
Root Port	: 0
Reconfig Counts	: 0
Topology Up Time	: 680904 (0 day 1 hr 53 min 29 sec)
 <OK> <Enter> to select.	

Parameter	Description
Priority	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.
Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Hold Time	The minimum interval between the transmission of consecutive Configuration BPDUs.
Designated Root	The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
Root Cost	The path cost from the root port on this switch to the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
Reconfig Counts	The number of times the Spanning Tree has been reconfigured.
Topology Up Time	The time since the Spanning Tree was last reconfigured.

Displaying the Current STA for Ports

The parameters shown in the following figure and table are for port STA Information.

Spanning Tree Port Information : Unit 1 Port 1 - 12					
=====					
Port	Type	Status	Designated Cost	Designated Bridge	Designated Port
1	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.1
2	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.2
3	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.3
4	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.4
5	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.5
6	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.6
7	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.7
8	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.8
9	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.9
10	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.10
11	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.11
12	10/100TX	NO LINK	0	32768.0010B5FD84BB	128.12

<OK>

<PREV UNIT>

<NEXT UNIT>

<PREV PAGE>

<NEXT PAGE>

Return to previous panel.

Use <TAB> or arrow keys to move. <Enter> to select.

Parameter	Description
Type	Shows port type as: 10/100TX: 10BASE-T / 100BASE-TX 100FX: 100BASE-FX 1000SX: 1000BASE-SX 1000LX: 1000BASE-LX
Status	Displays current state of this port within the Spanning Tree: No Link No link has been established on this port. Disabled Port has been disabled by the user or has failed diagnostics. Blocking Port receives STA configuration messages, but does not forward packets. Listening Port will leave blocking state due to topology change, starts transmitting configuration messages, but does not yet forward packets. Learning Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. Forwarding The port forwards packets, and continues learning addresses. The rules defining port status are: - A port on a network segment with no other STA-compliant bridging device is always forwarding. - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked. - All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
Designated Cost	The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.

Parameter	Description
Designated Bridge (ID)	The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
Designated Port (ID)	The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.

Using a Mirror Port for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a network sniffer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be included in the same VLAN as the source port. (See “Configuring Virtual LANs” on page 2-40.)

You can use the Mirror Port Configuration screen to designate a single port pair for mirroring as shown below.

```

Mirror Port Configuration
=====

Mirror Source Port : Unit 1
                   Port 1

Mirror Target Port : Unit 1
                   Port 2

Status              : DISABLED

<APPLY>             <OK>             <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Mirror Source Port	The port whose traffic will be monitored.
Mirror Target Port	The port that will duplicate or “mirror” all the traffic happening on the monitored port.
Status	Enables or disables the mirror function.

Configuring Port Trunks

Port trunks can be used to increase the bandwidth of a network connection or to ensure fault recovery. You can configure up to five trunk connections (combining 2~4 ports into a fat pipe) between any two standalone CheetahSwitch Workgroup-3726M switches, or up to 12 for an entire stack. However, before making any physical connections between devices, use the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, note that:

- The ports used in a trunk must all be of the same media type (RJ-45, 100 Mbps fiber, 1000BASE-SX or 1000BASE-LX). The ports that can be assigned to the same trunk have certain other restrictions as described on page 2-33.
- Ports can only be assigned to one trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including speed, duplex mode, and VLAN assignments.
- None of the ports in a trunk can be configured as a mirror source port or mirror target port.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.
- Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a loop.

You can use the Port Trunking Configuration screen to set up port trunks as shown below:

Port Trunking Configuration
=====

Trunk ID	Status	Member List			
		1	2	3	4
-----	-----	-----	-----	-----	-----
--	-----	Unit : -	Unit : -	Unit : -	Unit : -
		Port : --	Port : --	Port : --	Port : --
--	-----	Unit : -	Unit : -	Unit : -	Unit : -
		Port : --	Port : --	Port : --	Port : --
--	-----	Unit : -	Unit : -	Unit : -	Unit : -
		Port : --	Port : --	Port : --	Port : --
Trunk ID : 1		Trunk ID : 1		Member Unit : 1	
[Show]	[More]			Member Port : 1	
[Enable]	[Disable]		[Add]	[Delete]	
<OK>					
Use <TAB> or arrow keys to move, other keys to make changes.					

Parameter	Description
Trunk ID	Configure up to five trunks per switch.
Status	Shows if the selected trunk is enabled or disabled.
Unit	Specifies a switch unit in the stack (1~4).
Port	Select from 2 ~ 4 ports per trunk.
[Show]	Displays trunk settings, where the first trunk listed is specified by "Trunk ID."
[More]	Scrolls through the list of configured trunks.
[Enable] [Disable]	Enables/disables the selected trunk.
[Add] [Delete]	Adds/deletes the port specified by Trunk ID / Member Unit / Member Port.

The RJ-45 ports used for one side of a trunk must all be on the same internal switch chip. The port groups permitted include:

Group 1	Group 2	Group 3
1, 2, 3, 4, 13, 14, 15, 16	5, 6, 7, 8, 17, 18, 19, 20	9, 10, 11, 12, 21, 22, 23, 24

The 100BASE-FX fiber ports used for one side of a trunk must all be on the same module. However, the 1000BASE-SX and 1000BASE-LX ports used for one side of a trunk may be on any switch in the stack, or both on the same switch if used standalone.

Media Module

100BASE-FX	Any ports on a single module.
1000BASE-SX	Up to four Gigabit ports from any switch in the stack, or both Gigabit ports on two modules installed in a standalone switch.
1000BASE-LX	

For example, when using Gigabit ports to form a trunk within a stack, the Gigabit ports will all be at Port 25. In this case, you could specify a trunk group consisting of: (Unit1-Port25, Unit2-Port25, Unit3-Port25, Unit4-Port25), or two trunks consisting of: (Unit1-Port25, Unit2-Port25) and (Unit3-Port25, Unit4-Port25).

IGMP Multicast Filtering

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts which want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The switch looks up the IP Multicast Group used for this service and adds any port which received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. (For more information, see "IGMP Protocol" on page 4-5.)

Configuring IGMP

This protocol allows a host to inform its local switch/router that it wants to receive transmissions addressed to a specific multicast group. You can use the IGMP Configuration screen to configure multicast filtering shown below.

IGMP Configuration
=====

IGMP Status

:

ENABLED

IGMP Query Count

:

2

IGMP Report Delay (Seconds)

:

10

<APPLY>

<OK>

<CANCEL>

Use <TAB> or arrow keys to move. <Enter> to select

Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping.
IGMP Query Count	The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports. (Range 2 - 10.)
IGMP Report Delay	The time (in seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out that port and removes the entry from its list. (Range 5 - 30.)

Note: The default values are indicated in the sample screen.

Configuring Broadcast Storm Control

Use the Broadcast Storm Control Configuration screen to enable broadcast storm control for any port on the switch, as shown below.

```

Broadcast Storm Control Configuration : Unit 1 Port 1 - 12
=====

Broadcast control on all ports :      [Enable]  [Disable]
Port      Threshold      Broadcast Control
-----
1          500            ENABLED
2          500            ENABLED
3          500            ENABLED
4          500            ENABLED
5          500            ENABLED
6          500            ENABLED
7          500            ENABLED
8          500            ENABLED
9          500            ENABLED
10         500            ENABLED
11         500            ENABLED
12         500            ENABLED

<APPLY> <OK> <CANCEL> <PREV UNIT> <NEXT UNIT> <PREV PAGE> <NEXT PAGE>
      Enable Broadcast Control of all ports.
      Use <TAB> or arrow keys to move. <Enter> to select

```

Parameter	Description
Broadcast control on all ports	Allows you to enable/disable broadcast storm control for all ports on the switch. Select [Enable] and press <Enter> to enable broadcast control for all ports. Select [Disable] and press <Enter> to disable broadcast control for all ports.
Threshold	The packet-per-second threshold for broadcast packets on the port. (Default is 500 pps.)
Broadcast Control	Enables/disables broadcast control for the port. When enabled, the switch will employ a broadcast-control mechanism if the packet-per-second threshold is exceeded. This mechanism limits the amount of broadcasts passed by the port to half of the received packet-per-second count. The control mechanism remains in effect until the number of received broadcasts falls back below the packet-per-second threshold. (Default is Enabled.)

Configuring Bridge MIB Extensions

The Bridge MIB includes extensions for managed devices that support Traffic Classes and Virtual LANs. To display and configure these extensions, use the Extended Bridge Configuration screen as shown below.

```
Extended Bridge Configuration
=====

Bridge Capability : (Read Only)
Extended Multicast Filtering Services : NO
Traffic Classes : YES
Static Entry Individual Port : YES
VLAN Learning : SVL
Configurable PVID Tagging : YES
Local VLAN Capable : NO

Bridge Settings :
Traffic Classes : TRUE
GMRP : DISABLED
GVRP : DISABLED

<APPLY>          <OK>          <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Parameter	Description
<i>Bridge Capability</i>	
Extended Multicast Filtering Services	This switch does not support filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
Traffic Classes	This switch provides mapping of user priorities to multiple traffic classes. (Refer to "802.1P Port Traffic Class Information" on page 2-39.)
Static Entry Individual Port	This switch allows static filtering for unicast and multicast addresses. (Refer to Network Monitor Menu / Static Unicast Address Table Configuration and Static Multicast Address Table Configuration.)
VLAN Learning	This switch uses Shared VLAN Learning (SVL), whereby each port maintains its own VLAN filtering database.
Configurable PVID Tagging	This switch allows you to override the default PVID (Port VLAN ID) assigned to untagged incoming frames under "802.1Q VLAN Port Configuration" on page 2-44.
Local VLAN Capable	This switch does not support multiple local bridges (that is, multiple Spanning Trees).
<i>Bridge Settings</i>	
Traffic Class*	Multiple traffic classes are supported by this switch as indicated under Bridge Capabilities. However, you can disable this function by setting this parameter to False.
GMRP*	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. IGMP Snooping is currently used by this switch to provide multicast filtering.
GVRP*	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLANs groups which extend beyond the local switch.

* Not enabled in this firmware release.

Configuring Traffic Classes

IEEE 802.1P defines up to 8 separate traffic classes. This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. You can use the 802.1P Configuration menu to configure the default priority for each port, or to display the mapping for the traffic classes as described in the following sections.

802.1P Configuration
=====

802.1P Port Priority Configuration ...
802.1P Port Traffic Class Information ...

<OK>
Use <TAB> or arrow keys to move. <Enter> to select.

Port Priority Configuration

Inbound frames that do not have any VLAN tags are tagged with the input port's default VLAN ID (PVID) and the Default Ingress User Priority as shown in the following menu, and then sorted into the appropriate priority queue at the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority queue of the output port. You can use the following menu to adjust default ingress priority for any port as shown below.

802.1P Port Priority Configuration : Unit 1 Port 1 - 12		

Port	Default Ingress User Priority	Number of Egress Traffic Class

1	0	2
2	0	2
3	0	2
4	0	2
5	0	2
6	0	2
7	0	2
8	0	2
9	0	2
10	0	2
11	0	2
12	0	2
 <APPLY> <OK> <CANCEL> <PREV UNIT> <NEXT UNIT> <PREV PAGE> <NEXT PAGE> Use <TAB> or arrow keys to move, other keys to make changes.		

Parameter	Description
Port	Numeric identifier for switch port.
Default Ingress User Priority	Default ingress priority can be set to any value from 0~7, where 0~3 specifies the low priority queue and 4~7 specifies the high priority queue.
Number of Egress Traffic Classes	Indicates that this switch supports two priority output queues.

802.1P Port Traffic Class Information

This switch provides two priority levels with Weighted Fair Queuing for port egress. This means that any frames with a priority tag from 0~3 are sent to the low priority queue "0" while those from 4~7 are sent to the high priority queue "1" as shown in the following screen.

802.1P Port Traffic Class Information : Unit 1 Port 1 - 12								
=====								
Port	User Priority							
	0	1	2	3	4	5	6	7

1	0	0	0	0	1	1	1	1
2	0	0	0	0	1	1	1	1
3	0	0	0	0	1	1	1	1
4	0	0	0	0	1	1	1	1
5	0	0	0	0	1	1	1	1
6	0	0	0	0	1	1	1	1
7	0	0	0	0	1	1	1	1
8	0	0	0	0	1	1	1	1
9	0	0	0	0	1	1	1	1
10	0	0	0	0	1	1	1	1
11	0	0	0	0	1	1	1	1
12	0	0	0	0	1	1	1	1
<OK> <PREV UNIT> <NEXT UNIT> <PREV PAGE> <NEXT PAGE> Use <TAB> or arrow keys to move. <Enter> to select.								

Parameter	Description
Port	Numeric identifier for switch port.
User Priority	Shows that user priorities 0~3 specify the low priority queue and 4~7 specify the high priority queue.

Configuring Virtual LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 256 LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBeui. By using IEEE 802.1Q compliant VLANs, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, see "Virtual LANs" on page 4-2. The VLAN configuration screens are described in the following sections.

802.1Q VLAN Base Information

The 802.1Q VLAN Base Information screen displays basic information on the VLAN type supported by this switch.

```

                                802.1Q VLAN Base Information
                                =====

VLAN Version Number              : 1

MAX VLAN ID                      : 2048

MAX Supported VLANs              : 256

Current Number of 802.1Q VLANs Configured : 1

                                <OK>
                                <Enter> to select.
```

Parameter	Description
VLAN Version Number	The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
MAX VLAN ID	Maximum VLAN ID recognized by this switch.
MAX Supported VLANs	Maximum number of VLANs that can be configured on this switch.
Current Number of VLANs Configured	The number of VLANs currently configured on this switch.

802.1Q VLAN Current Table Information

This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports to the same untagged VLAN. The current configuration is shown in the following screen.

```

< 802.1Q VLAN Current Table Information >

Deleted VLAN Entry Counts : 0

VID                Creation Time                Status
-----
1          0 (0 day 0 hr 0 min 0 sec)          Permanent

Unit  Current Egress Ports                Current Untagged Ports
1.    111111111111 111111111111 11--  111111111111 111111111111 11--
2.    -----
3.    -----
4.    -----

Sorted by VID : 1

[Show]    [More]

Port 1 Port 13 Port 25

<Ok>
Use <TAB> or arrow keys to move. <Enter> to select

```

Parameter	Description
Deleted VLAN Entry Counts	The number of times a VLAN entry has been deleted from this table.
VID	The ID for the VLAN currently displayed.
Creation Time	The value of sysUpTime (System Up Time) when this VLAN was created.
Status	Shows how this VLAN was added to the switch. Dynamic GVRP: Automatically learned via GVRP. Permanent: Added as a static entry.
Unit	Stack unit.
Current Egress Ports	Shows the ports which have been added to the displayed VLAN group, where "1" indicates that a port is a member and "0" that it is not.
Current Untagged Ports	If a port has been added to the displayed VLAN (see Current Egress Ports), its entry in this field will be "1" if the port is untagged or "0" if tagged.
Sorted by VID	The VLAN ID number from which the display will start.
[Show]	Displays the members for the VLAN indicated by the "Sorted by VID" field.
[More]	Displays any subsequent VLANs if configured.

802.1Q VLAN Static Table Configuration

Use this screen to create a new VLAN or modify the settings for an existing VLAN. You can add/delete port members for a VLAN from any unit in the stack as a tagged or untagged member. Or you can prevent a port from being automatically added to a VLAN by the GVRP protocol.

```

      802.1Q VLAN Static Table Configuration
      =====
      VID      VLAN Name      Status
      -----
      1              Active

Unit  Egress Ports              Forbidden Egress Ports
1.    111111111111 111111111111 11--  00000000000000 00000000000000 00--
2.    -----
3.    -----
4.    -----

Unit  Untagged Ports              VID : 1
1.    111111111111 111111111111 11--  [Show]
2.    -----
3.    ----- [More]
4.    ----- [New]

      <APPLY>          <OK>          <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
VID	The ID for the VLAN currently displayed. Range: 1-2048
VLAN Name	A user-specified symbolic name for this VLAN. String length: Up to 8 alphanumeric characters
Status	Sets the current editing status for this VLAN as: Not in Service, Destroy or Active.
Unit	Stack unit.
Egress Ports	Set the entry for any port in this field to "1" to add it to the displayed VLAN, or "0" to remove it from the VLAN.
Forbidden Egress Ports	Prevents a port from being automatically added to this VLAN via GVRP. Note that GVRP is not supported in the current firmware release.
Untagged Ports	You can add a port to the displayed VLAN as an untagged port by setting this field to "1" or as a tagged port by setting it to "0." This field is only enabled if the corresponding port has been added to the displayed VLAN as an "Egress Port."
[Show]	Use <TAB> or the arrow keys to select this field, then press <Enter> to display settings for the VLAN specified in the VID field immediately above.
[More]	Use <TAB> or the arrow keys to select this field, then press <Enter> to display the next consecutively numbered VLAN.
[New]	Use <TAB> or the arrow keys to select this field, then press <Enter> to set up the screen for configuring a new VLAN.

For example, the following screen displays settings for VLAN 2, which includes untagged ports 1-6, and forbidden port 8.

```

                        802.1Q VLAN Static Table Configuration
                        =====
VID      VLAN Name      Status
-----
      2                      Active

Unit  Egress Ports
1.    111111000000 000000000000 00-- 0000000010000 000000000000 00--
2.    -----
3.    -----
4.    -----
Unit  Untagged Ports
1.    111111000000 000000000000 00-- VID : 2
2.    ----- [Show]
3.    ----- [More]
4.    ----- [New]

      <Apply>                <Ok>                <Cancel>
Use <TAB> or arrow keys to move, other keys to make changes.

```

- Notes:**
1. To allow this switch to participate in a VLAN group that extends beyond this switch, you must add the VLAN ID for the required external groups.
 2. If a removed port is no longer assigned to any other group as an untagged port, it will automatically be assigned to VLAN group 1 as untagged.

802.1Q VLAN Port Configuration

Use this screen to configure port-specific settings for IEEE 802.1Q VLAN features.

802.1Q VLAN Port Configuration : Unit 1 Port 1 - 12

=====

Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GVRP Failed Registrations	GVRP Last PDU Origin
1	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
2	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
3	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
4	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
5	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
6	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
7	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
8	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
9	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
10	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
11	1	All	FALSE	DISABLED	0	00-00-00-00-00-00
12	1	All	FALSE	DISABLED	0	00-00-00-00-00-00

<APPLY> <OK> <CANCEL> <PREV UNIT> <NEXT UNIT> <PREV PAGE> <NEXT PAGE>
Use <TAB> or arrow keys to move, other keys to make changes.

Parameter	Description
PVID	The VLAN ID assigned to untagged frames received on this port.
Acceptable Frame Type ¹	This switch accepts "All" frame types, including VLAN tagged or VLAN untagged frames. Note that all VLAN untagged frames received on this port are assigned to the PVID for this port.
Ingress Filtering ¹	If set to "True," incoming frames for VLANs which do not include this ingress port in their member set will be discarded at the ingress port.
GVRP Status ²	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. Note that GVRP must be enabled for the switch before this setting can take effect. (See Device Control Menu / Extended Bridge Configuration.)
GVRP Failed Registrations ²	The total number of failed GVRP registrations, for any reason, on this port.
GVRP Last PDU Origin ²	The Source MAC Address of the last GVRP message received on this port.

1: These controls do not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

2: Not available for the current firmware release.

Port Security Configuration

Use the Port Security Configuration screen to enable and configure port security for the switch. Port Security allows you to configure each port with a list of MAC addresses of devices that are authorized to access the network through that port.

Port Security Configuration
=====

MAC Address

MAC Address

Secure address count : 0

Unit : 1

Port : 1

MAC : 00-00-00-00-00-00

[Show]

[More]

[Add]

[Delete]

Mode:DISABLE

[Apply]

[Clear]

<OK>

Use <TAB> or arrow keys to move. <Enter> to select

Parameter	Description
MAC Address	A list of the authorized MAC addresses that can access the network through the specified port.
Secure Address Count	The number of authorized MAC addresses for the specified port.
Unit	The stack unit ID.
Port	The port number on the unit.
[Show]	Displays authorized MAC addresses for the specified port.
[More]	Displays more MAC addresses for the port.
Mode	Port security can be set to three states; Static, Disable, or Learning. When set to Static, the switch will drop packets from the port if the source MAC address does not match one of the addresses in the MAC Address list. If set to Learning, the switch will add the source MAC address of all packets received on the port to the authorized MAC Address list.
[Apply]	Applies a change of Mode to the port.
MAC	A specific MAC address to be added or deleted from the list.
[Add]	Adds a new MAC address to the current list.
[Delete]	Removes a MAC address from the current list.
[Clear]	Clears all the MAC addresses for the current port.

Monitoring the Switch

The Network Monitor Menu provides access to port statistics, RMON statistics, IP multicast addresses, and the static address table. Each of the screens provided by these menus is described in the following sections.

```

                                Network Monitor Menu
                                =====

Port Statistics ...
RMON Statistics ...
Unicast Address Table ...
Multicast Address Registration Table ...
IP Multicast Registration Table ...
Static Unicast Address Table Configuration ...
Static Multicast Address Table Configuration...

                                <OK>
Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full listing of all unicast addresses stored in the switch, as well as sort, search and clear functions.
Multicast Address Registration Table*	Displays the ports that belong to each GMRP Multicast group.
IP Multicast Registration Table	Displays the ports that belong to each IP Multicast group.
Static Unicast Address Table Configuration	Allows you to display or configure static unicast addresses.
Static Multicast Address Table Configuration*	Allows you to display or configure static GMRP multicast addresses.

* Not implemented in this firmware release.

Displaying Port Statistics

Port Statistics display key statistics from the Ethernet-like MIB for each port. Error statistics on the traffic passing through each port are displayed. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). The values displayed have been accumulated since the last system reboot.

Select the required port. The statistics displayed are indicated in the following figure and table.

Port Statistics : Unit 1 Port 1	
=====	
Ether Like Counter :	
Alignment Errors	: 0
FCS Errors	: 0
Single Collision Frames	: 0
Multiple Collision Frames	: 0
SQE Test Errors	: 0
Deferred Transmissions	: 0
Late Collisions	: 0
Excessive Collisions	: 0
Internal Mac Transmit Errors	: 0
Carrier Sense Errors	: 0
Frame Too Longs	: 0
Internal Mac Receive Errors	: 0
[Refresh Statistics]	Show port : 1
[Reset Counters]	[Show]
<OK> <PREV UNIT> <NEXT UNIT> <PREV PORT> <NEXT PORT> Use <TAB> or arrow keys to move. <Enter> to select	

Menu	Description
FCS Errors	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames*	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames*	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
SQE Test Errors*	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions*	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions*	The number of frames for which transmission failed due to excessive collisions.
Internal Mac Transmit Errors*	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carrier Sense Errors*	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frames Too Long	The number of frames received that exceed the maximum permitted frame size.

Menu	Description
Internal Mac Receive Errors	The number of frames for which reception failed due to an internal MAC sublayer receive error.

* The reported values will always be zero because these statistics are not supported by the internal chip set.

Note: Statistics are automatically refreshed every 5 seconds (see page 2-14).

Displaying RMON Statistics

Use the RMON Statistics screen to display key statistics for each port from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software.) The following screen displays the overall statistics on traffic passing through each port. RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. Values displayed have been accumulated since the last system reboot.

```

RMON Statistics : Unit 1 Port 1
=====

Drop Events      : 0                Jabbers          : 0
Received Bytes   : 0                Collisions       : 0
Received Frames  : 0                64 Byte Frames   : 0
Broadcast Frames : 0                65-127 Byte Frames : 0
Multicast Frames : 0                128-255 Byte Frames : 0
CRC/Alignment Errors : 0           256-511 Byte Frames : 0
Undersize Frames : 0                512-1023 Byte Frames : 0
Oversize Frames  : 0                1024-1518 Byte Frames : 0
Fragments        : 0

[Refresh Statistics]                Show port : 1
[Reset Counters]                   [Show]

<OK>    <PREV UNIT>  <NEXT UNIT>    <PREV PORT>  <NEXT PORT>
          Use <TAB> or arrow keys to move. <Enter> to select

```

Menu	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Frame Errors	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.

Menu	Description
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames	The total number of frames (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Note: Statistics are automatically refreshed every 5 seconds (see page 2-14).

Displaying the Unicast Address Table

The Address Table contains the MAC addresses and VLAN identifier associated with each port (that is, the source port associated with the address and VLAN), sorted by MAC address or VLAN ID. You can search for a specific address, clear the entire address table, or information associated with a specific address, or set the aging time for deleting inactive entries. The information displayed in the Address Table is indicated in the following figure and table.

Unicast Address Table									
=====									
Aging Time : 300		Dynamic Counts : 173				Static Counts : 0			
MAC	VID	Unit	Port	Status	MAC	VID	Unit	Port	Status

00-00-11-11-43-29	1	1	24	D	00-00-E8-00-00-03	1	1	24	D
00-00-E2-12-F9-F8	1	1	24	D	00-00-E8-00-00-07	1	1	24	D
00-00-E2-16-C5-82	1	1	24	D	00-00-E8-00-00-08	1	1	24	D
00-00-E2-20-C3-D5	1	1	24	D	00-00-E8-00-00-96	1	1	24	D
00-00-E2-21-74-D0	1	1	24	D	00-00-E8-00-01-01	1	1	24	D
00-00-E2-2A-59-9A	1	1	24	D	00-00-E8-07-12-5E	1	1	24	D
00-00-E2-2E-FD-F6	1	1	24	D	00-00-E8-11-11-33	1	1	24	D
00-00-E8-00-00-02	1	1	24	D	00-00-E8-12-12-12	1	1	24	D
Sorted by : MAC + VID					Cleared by : MAC + VID				
VLAN ID : 1					VLAN ID : 1				
MAC : 00-00-00-00-00-00					MAC : 00-00-00-00-00-00				
[Show] [More]					[Clear] [Clear Dynamic]				
<Apply>			<Ok>			<Cancel>			
Use <TAB> or arrow keys to move, other keys to make changes.									

Menu	Description
Aging Time	Time-out period in seconds for aging out dynamically learned forwarding information. Range: 10 - 415 seconds; Default: 300 seconds
Dynamic Count	The number of dynamically learned addresses in the table.
Static Count	The number of static addresses in the table.
MAC	The MAC address of a node.
VID	The VLAN(s) associated with this address or port.
Unit	Switch unit in the stack (1~6).
Port	The port whose address table includes this MAC address.
Status	Indicates address status as: D: Dynamically learned, or P: Fixed permanently by SNMP network management software.
Sorted/Cleared by	Selects the primary key used to sort/clear the table: MAC or VID.
[Show]	Displays the address table according to the settings on the left-hand side of the screen. Use <TAB> or the arrow keys to select the "Sorted by" field, then use the <Space bar> to select the primary sort key, MAC or VID. In the VLAN ID field, set the VLAN at which you want the table listing to start. In the MAC field, set the MAC address at which you want the table listing to start. Select the [Show] field and press <Enter> to display the table entries.
[More]	Use <TAB> or the arrow keys to select this field, then press <Enter> to scroll through the next page of address table entries for the current settings on the left-hand side of the screen.

Menu	Description
[Clear]	Clears address table entries according to the settings on the right-hand side of the screen. Use <TAB> or the arrow keys to select the "Cleared by" field, then use the <Space bar> to select the primary key, MAC or VID. In the VLAN ID field, set the ID to clear the table of all entries in a specific VLAN. In the MAC field, set a specific MAC address to clear from the table. Select the [Clear] field and press <Enter> to remove entries from the table.
[Clear Dynamic]	Use <TAB> or the arrow keys to select this field and press <Enter> to remove all dynamically learned MAC addresses from the table.

Displaying the IP Multicast Registration Table

Use the IP Multicast Registration Table to display all the multicast groups active on this switch, including multicast IP addresses and the corresponding VLAN ID.

IP Multicast Registration Table =====				
VID	Multicast IP	Unit	Multicast Group Port Lists	Learned by

		1.		
		2.		
		3.		
		4.		
		1.		
		2.		
		3.		
		4.		
Sorted by : VID + Multicast IP				
VID : 1				
Multicast IP :				
[Show] [More]				
<OK>				
Use <TAB> or arrow keys to move. <Enter> to select				

Menu	Description
VID	VLAN ID assigned to this multicast group.
Multicast IP	IP address for specific multicast services.
Unit	Stack unit.
Dynamic Port Lists	The switch ports registered for the indicated multicast service.
Learned by	Indicates the manner in which this address was learned: Dynamic or IGMP.
Sorted by	Selects the primary sort key for displaying table entries. Note that only VID+Multicast IP is implemented in the current firmware release.
[Show]	Displays the address table sorted on VID and then Multicast IP.
[More]	Scrolls through the entries in the address table.

Configuring Static Unicast Addresses

Use the Static Unicast Address Table Configuration screen to manually configure host MAC addresses in the unicast table. You can use this screen to associate a MAC address with a specific VLAN ID and switch port as shown below.

Static Unicast Address Table Configuration
=====

VID	MAC Address	Unit	Port	Status

Sorted by : VID + MAC
VID : 1
MAC : 00-00-00-00-00-00

VID : 1 Unit : 1 MAC : 00-00-00-00-00-00
Unit : 1 Port : 1
Status : Permanent

[Show] [More] [Set]

<OK>
Use <TAB> or arrow keys to move. <Enter> to select

Menu	Description
VID	The VLAN group this port is assigned to.
MAC Address	The MAC address of a host device attached to this switch.
Unit	The switch unit the host device is attached to.
Port	The port the host device is attached to.
Status	The status for an entry can be set to: Permanent This entry is currently in use and will remain so after the next reset of the switch. DeleteOnReset This entry is currently in use and will remain so until the next reset. Invalid Removes the corresponding entry. DeleteOnTimeOut This entry is currently in use and will remain so until it is aged out. (Refer to "Aging Time" on page 2-50.) Other This entry is currently in use but the conditions under which it will remain so differ from the preceding values.
Sorted by	Selects the primary sort key for displaying table entries. Note that only VID+MAC is implemented in the current firmware release.
[Show]	Displays the static address table sorted on VID as the primary key and MAC address as secondary key.
[More]	Scrolls through entries in the static address table.
[Set]	Adds the specified entry to the static address table, such as shown in the following example: VID : 1 MAC : 00-00-00-e8-34-22 Unit : 1 Port : 1 Status : Permanent

Resetting the System

Use the Restart command under the Main Menu to reset the management agent. The reset screen includes options as shown in the following figure and table.

```

                        System Restart Menu
                        =====

Restart Option :

      POST                      : YES
      Reload Factory Defaults   : NO
      Keep IP Setting           : NO
      Keep User Authentication   : NO

      [Restart]

      <APPLY>          <OK>          <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Menu	Description
POST	Runs the Power-On Self-Test
Reload Factory Defaults	Reloads the factory defaults
Keep IP Setting	Retains the settings defined in the IP Configuration menu.
Keep User Authentication	Retains the user names and passwords defined in the Console Login Configuration menu.
[Restart]	Restarts the switch.

Logging Off the System

Use the Exit command under the Main Menu to exit the configuration program and terminate communications with the switch for the current session.

Chapter 3: Web-Based Management

Web-Based Configuration and Monitoring

As well as the menu-driven system configuration program, the agent module provides an embedded HTTP Web agent. This agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above).

Using the Web browser management interface you can configure a switch and view statistics to monitor network activity. The Web interface also provides access to a range of SNMP management functions with access to the switch's MIB and RMON database.

Prior to accessing the switch from a Web browser, be sure you have first performed the following tasks:

1. Configure it with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection or BOOTP protocol.
2. Set the Administrator user name and password using an out-of-band serial connection. Access to the Web agent is controlled by the same Administrator user name and password as the on-board configuration program.

Navigating the Web Browser Interface

To access the Web-browser interface you must first enter a user name and password. The default user name is “admin,” with no password.” The administrator has Read/Write access to all configuration parameters and statistics.

Home Page

When your Web browser connects with the switch's Web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left-hand side of the screen and System Information on the right-hand side. The Main Menu links are used to navigate to other menus and display configuration parameters and statistical data.

The screenshot shows the Accton CheetahSwitch Workgroup 3726M Manager web interface. The header includes the Accton logo, a status bar with 'Link Up' and 'Link Down' indicators, and a 'Unit: 1' dropdown. The main menu on the left lists various system functions. The main content area displays system information for 'CheetahSwitch Workgroup 3726M Manager'.

CheetahSwitch Workgroup 3726M Manager	
System Name	DEFAULT SYSTEM NAME
IP Address	10.2.13.19
Object ID	1.3.6.1.4.1.259.6.10.34
Location	DEFAULT SYSTEM LOCATION
Contact	DEFAULT SYSTEM CONTACT
System Up Time	0 d 0 h 1 min 33 s

Below the system information, there are three links: 'Telnet' (Connect to textual user interface), 'Support' (Send mail to technical support), and 'Contact' (Connect to Accton Web page). At the bottom, there are 'Apply', 'Revert', and 'Help' buttons.

If this is your first time to access the management agent, you should define a new Administrator password, record it and put it in a safe place. From the Main Menu, select Security and enter a new password for the Administrator. Note that passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

Note: Based on the default configuration, a user is allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated. See “Console Login Configuration” on page 2-18.

Configuration Options

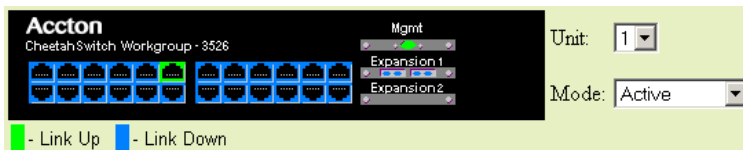
Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the “Apply” button at the bottom of the page to confirm the new setting. The following table summarizes the Web page configuration buttons.

Web Page Configuration Buttons	
Button	Action
Apply	Sets specified values in the management agent.
Revert	Cancels specified values prior to pressing the “Apply” button.
Refresh	Immediately updates values from the management agent.
Help	Provides help on using the Web management interface.

- Notes:**
1. To ensure proper screen refresh, be sure that Internet Explorer 5.0 is configured as follows: Under the menu “Tools / Internet Options / General / Temporary Internet Files / Settings,” the setting for item “Check for newer versions of stored pages” should be “Every visit to the page.”
 2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser’s refresh button.

Panel Display

The Web agent displays an image of the switch’s ports, showing port links and activity. Clicking on the image of a port displays statistics and configuration information for the port. Clicking on the image of the management module display displays the Console Configuration screen.



Port State Display

Click on any port to display a summary or port status as shown below, as well as Etherlike statistics (page 3-42) and RMON statistics (page 3-43).

Type	10Base-T / 100Base-TX
Admin Status	Enabled
Link Status	Down
Speed Status	10M
Duplex Status	Half
Flow Control Status	Disabled
VLAN	1

Parameter	Description
Type	Shows port type as: 10/100TX: 10BASE-T / 100BASE-TX
Admin Status	Shows if the port is enabled, or has been disabled due to abnormal behavior or for security reasons. See "Port Configuration" on page 3-34.
Link Status	Indicates if the port has a valid connection to an external device.
Speed Status	Indicates the current port speed.
Duplex Status	Indicates the port's current duplex mode.
Flow Control Status	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch.
VLAN	The VLAN ID assigned to untagged frames received on this port. You can set the default Port VLAN ID (PVID) under "VLAN Port Configuration" on page 3-30 to assign ports to the same untagged VLAN.

Console Configuration

If you are having difficulties making an out-of-band console connection to the serial port on the agent module, you can display or modify the current settings for the serial port through the Web agent. Click on the management module icon in the switch image to display or configure these settings, as shown below.

Baud rate	19200 ▼
Time-Out	0 minutes
Data bits	8 ▼
Stop bits	1 ▼
Parity	None ▼
Auto-Refresh Time	5 seconds

Parameter	Default	Description
Baud rate	19200 bps	The rate at which data is sent between devices. Options : 2400, 4800, 9600, 19200, and auto detection. Note that when AUTO is selected, you need to first press the Enter key once to set the data rate and initialize the connection.
Time-Out	10 minutes	If no input is received from the attached device after this interval, the current session is automatically closed. Range : 0 - 100 minutes; 0: disabled
Data bits	8 bits	Sets the data bits of the RS-232 port. Options : 7, 8
Stop bits	1 bit	Sets the stop bits of the RS-232 port. Options : 1, 2
Parity	none	Sets the parity of the RS-232 port. Options : none/odd/even
Auto-Refresh Time	5 seconds	Sets the interval before a console session will auto refresh the console information, such as Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. Range : 5-255 seconds; 0: disabled

Main Menu

Using the on-board Web agent, you can define system parameters, manage and control the switch, the connected stack and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Menu	Description
System	Provides basic system description, including contact information.
Switch	Shows hardware/firmware version numbers, power status, and expansion modules in use.
IP	Includes boot state, IP address, and the maximum number of Telnet sessions allowed.
SNMP	Configures communities and trap managers; and activates traps.
Security	Sets password for system access.
Upgrade	Downloads new version of firmware to update your system.
Configure	Saves the switch configuration to a file on a TFTP server. This file can be later downloaded to restore the configuration.
Address Table	Provides full listing of unicast addresses, sorted by address or VLAN.
STA	Enables Spanning Tree Algorithm; also sets parameters for switch priority, hello time, maximum message age, and forward delay; as well as port priority and path cost.
Bridge Extension	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes and VLAN extensions.
Priority	Configures default port priorities and displays queue assignments.
VLAN	Configures VLAN group members and other port-specific VLAN settings.
IGMP	Configures IGMP multicast filtering.
Port	Enables any port, sets communication mode to auto-negotiation, full duplex or half duplex, and enables/disables flow control. Also configures broadcast storm control and port security.
Mirror	Sets the source and target ports for mirroring.
Trunk	Specifies ports to group into aggregate trunks.
Statistics	Displays statistics on network traffic passing through the selected port.

System Information

Use the System Information screen to display descriptive information about the switch, or for quick system identification as shown in the following figure and table.

System Name	DEFAULT SYSTEM NAME
IP Address	10.2.13.19
Object ID	1.3.6.1.4.1.259.6.10.34
Location	DEFAULT SYSTEM LOCATION
Contact	DEFAULT SYSTEM CONTACT
System Up Time	0 d 0 h 5 min 54 s

Parameter	Description
System Name*	Name assigned to the switch system.
IP Address	IP address of the agent you are managing. The agent supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent (or running management software) must have an IP address. Valid IP addresses consist of four decimal numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Object ID	MIB II object identifier for switch's network management subsystem.
Location*	Specifies the area or location where the system resides.
Contact*	Contact person for the system.
System Up Time	Length of time the current management agent has been running.

* Maximum string length is 255, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

Switch Information

Use the Switch Information screen to display hardware/firmware version numbers for the main board, as well as the power status and modules plugged into the system.

Main Board

Serial Number	00-00-04-00-00-00
Number of Ports	26
Hardware Version	V3.0
Firmware Version	V1.29
Internal Power Status	Active
Redundant Power Status	Inactive

Parameter	Description
Serial Number	Serial number of the main board.
Number of Ports	Number of switch ports (including modules).
Hardware Version	Hardware version of the main board.
Firmware Version	Main board system firmware version in ROM.
Internal Power Status	Power status for the switch.
Redundant Power Status	Redundant power status for the switch.

Agent Module

Hardware Version	V3.0 (850 CPU)
POST ROM Version	V1.11
Firmware Version	V2.476
Role	Master

Parameter	Description
Hardware Version	Hardware version of the agent module.
POST ROM Version	Agent module's Power-On Self-Test version.
Firmware Version	Agent module's firmware version.
Role	Shows if this module is Master or Slave.

Expansion Slot

Expansion Slot 1	2-Port 100Base-FX-SC(MMF)
Expansion Slot 2	1-Port 1000Base-GBIC

Parameter	Description
Expansion Slot 1	Shows module type if inserted (100BASE-FX, 1000BASE-SX or 1000BASE-LX). 2-Port 100Base-FX-SC(MMF) : 100BASE-FX (multimode) 1-Port 1000Base-SX-SC : 1000BASE-SX (multimode) 1-Port 1000Base-LX-SC : 1000BASE-LX (singlmode)
Expansion Slot	Shows module type if inserted (100BASE-FX, 1000BASE-SX, 1000BASE-LX or Stacking). 2-Port 100Base-FX-SC(MMF) : 100BASE-FX (multimode) 1-Port 1000Base-SX-SC : 1000BASE-SX (multimode) 1-Port 1000Base-LX-SC : 1000BASE-LX (singlmode) Stacking Module

IP Configuration

Use the IP Configuration screen to set the bootup option, configure the IP address for the on-board management agent, or set the number or concurrent Telnet sessions allowed. The screen shown below is described in the following table.

IP State	User-Configured ▼
IP Address	10.2.13.15
Subnet Mask	255.255.252.0
Gateway IP Address	0.0.0.0
MAC Address	00-10-B5-FD-84-BB
Maximum Number of Telnet Sessions (1-4)	4

Parameter	Default	Description
IP State	USER-CONFIG	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BOOTP). Options include: USER-CONFIG - IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.) BOOTP Get IP - IP is enabled but will not function until a BOOTP reply has been received. BOOTP requests will be periodically broadcast by the switch in an effort to learn its IP address. (BOOTP values can include the IP address, default gateway, and subnet mask.)
IP Address	10.1.0.1	IP address of the switch you are managing. The switch supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the on-board agent (or running management software) are assigned an IP address. Valid IP addresses consist of four decimal numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	255.255.0.0	Subnet mask of the switch you have selected. This mask identifies the host address bits used for routing to specific subnets.
Gateway IP Address		Gateway used to pass trap messages from the switch to the management station. Note that the gateway must be defined if the management station is located in a different IP segment.
MAC Address		Physical address of the agent module.
Maximum Number of Telnet Sessions	4	Sets the number of concurrent Telnet sessions allowed to access the agent.

SNMP Configuration

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The stack should include an SNMP agent module which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent module are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following figures and table.

SNMP Community

The following figure and table describe how to configure the community strings authorized for management access. Up to 5 community names may be entered.

SNMP Community:

SNMP Community Capability: 5

Current:

public RW

<< Add

Remove

New:

Community String

Access Mode

Read-Only

Parameter	Description
SNMP Community Capability	Up to 5 community strings may be used.
Community String	A community entry authorized for management access. (The maximum string length is 20 characters.)
Access Mode	Management access is restricted to Read Only or Read/Write.
Add/Remove	Add/remove strings from the active list.

Trap Managers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.

Trap Manager Capability: 5

Current:	New:
(none) << Add Remove	Trap Manager IP address Trap Manager Community String

Enable Authentication Traps: ☒

Parameter	Description
Trap Manager Capability	Up to 5 trap managers may be used.
Trap Manager IP Address	IP address of the trap manager.
Trap Manager Community String	A community authorized to receive trap messages.
Add/Remove	Add/remove strings from the active list.
Enable Authentication Traps	Issues a trap message to specified IP trap managers whenever authentication of an SNMP request fails. Default: enabled

Security Configuration

Use the Security Configuration screen to restrict management access based on a specified password. The Administrator has write access for parameters governing the SNMP agent. You should therefore assign a password to the default Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you cannot gain access to the system's configuration program, contact Accton Technical Support for assistance.)

Change Password

Old Password	
New Password	
Confirm Password	

This password is for the system Administrator, with access privilege of Read/Write for all screens. Passwords can consist of up to 11 alphanumeric characters and are not case sensitive. (The default user name is "admin," with no password.)

Firmware Upgrade Options

You can upgrade system firmware via a Web browser, a TFTP server, or a direct connection to the console port.

Web Upload Management

Use the Web Upload Management menu to load software updates into the switch. The upload file should be an CheetahSwitch Workgroup-3726M binary file from Accton; otherwise the agent will not accept it. The success of the upload operation depends on the quality of the network connection. After uploading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

Upload Mode	Permanent	
File Name		Browse...

Start Web Upload

Parameter	Description
Upload Mode	Uploads to permanent flash ROM.
File Name	The binary file to download. Use the Browse button to locate the file on your local network.
Start Web Upload	Starts uploading the file over the network.

TFTP Download Management

Use the TFTP Download Management menu to load software updates into the switch. The download file should be an CheetahSwitch Workgroup-3726M binary file from Accton; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

Server IP Address	0.0.0.0
Download Mode	Permanent
File Name	

Start TFTP Download

Parameter	Description
Server IP Address	IP address of a TFTP server.
Download Mode	The system downloads to permanent flash ROM.
File Name	The binary file to download.
Start TFTP Download	Issues request to TFTP server to download the specified file.

Configuration Save and Restore

Use the Configure screen to save the switch configuration settings to a file on a TFTP server. The file can be later downloaded to the switch to restore the switch's settings. The success of the operation depends on the accessibility of the TFTP server and the quality of the network connection.

Configuration Upload Management

Use the Configuration Upload Management to save the switch configuration to a file on a TFTP sever. Parameters shown on this screen are indicated in the following figure and table.

Server IP Address	0.0.0.0
File Name	

Start Configuration TFTP Upload

Parameter	Description
Server IP Address	IP address of a TFTP server.
File Name	The name of the file to contain the switch configuration settings.
Start Configuration TFTP Upload	Issues a request to upload the configuration settings to the specified file on the TFTP server.

Configuration Download Management

Use the Configuration Download Management to restore switch configuration settings from a file on a TFTP sever. Parameters shown on this screen are indicated in the following figure and table.

Server IP Address	0.0.0.0
File Name	

Start Configuration TFTP Download

Parameter	Description
Server IP Address	IP address of a TFTP server.
File Name	The name of the file that contains the switch configuration settings you wish to restore.
Start Configuration TFTP Download	Issues a request to the TFTP server to download the specified file.

Address Table Configuration

The Address Table contains the unicast MAC addresses and VLAN identifier associated with each port (that is, the source port), sorted by MAC address or VLAN. You can also clear the entire address table, or information associated with a specific address; or set the aging time for deleting inactive entries. The information displayed in the Address Table is indicated in the following figure and table.

Aging Time (10-415):	300 seconds
Dynamic Address Counts:	1
Static Address Counts:	0

Address Table Sort Key: Address

Address Table:

00C00C-722321, VLAN 1, Unit 1, Port 6, Dynamic

New Static Address:

<< Add	MAC Address	
Remove	VLAN (1-2048)	
Clear Table	Unit	1
	Port	1

Parameter	Description
Aging Time	Time-out period in seconds for aging out dynamically learned forwarding information. Range: 10 - 415 secs; default: 300 secs.
Dynamic Address Counts	The number of dynamically learned addresses.
Static Address Counts	The number of statically configured addresses.
Address Table Sort Key	Entries can be sorted by address or VLAN ID.
Address Table	The system displays the MAC address of each node, and the port whose address table includes this MAC address, the associated VLAN(s), and the address status (i.e., dynamic or static).
New Static Address	Use these fields to add or remove a static entry to the address table. Indicate the address, stack unit, port and VLAN group when adding a new entry.
Add/Remove	Adds/removes the selected address.
Clear Table	Removes all addresses from the address table.

Spanning Tree Algorithm (STA)

The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network. For a more detailed description of how to use this algorithm, refer to “Spanning Tree Algorithm” on page 4-1.

Spanning Tree Information

The Spanning Tree Information screen displays a summary of the STA information for the overall bridge or for a specific port. To make any changes to the parameters for the Spanning Tree, use the Spanning Tree Configuration menu.

Spanning Tree

The parameters shown in the following figure and table describe the current bridge STA Information.

Spanning Tree State	Enabled	Designated Root	32768.0010B5FD84BB
Bridge ID	32768.0010B5FD84BB	Root Port	0
Max Age	20 seconds	Root Path Cost	0
Hello Time	2 seconds	Configuration Changes	0
Forward Delay	15 seconds	Last Topology Change	0 d 0 h 6 min 3 s

Parameter	Description
Spanning Tree State	Shows if the switch is enabled to participate in an STA-compliant network.
Bridge ID	A unique identifier for this bridge, consisting of bridge priority plus MAC address (where the address is normally taken from the agent).
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.
Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Designated Root	The priority and MAC address of the device in the spanning tree that this switch has accepted as the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the spanning tree network.
Root Path Cost	The path cost from the root port on this switch to the root device.
Configuration Changes	The number of times the spanning tree has been reconfigured.
Last Topology Change	The time since the spanning tree was last reconfigured.

Ports

The parameters shown in the following figure and table are for port STA Information.

Port	Port Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port
1	No Link	0	19	32768.0010B54C1EB6	128.1
2	No Link	0	19	32768.0010B54C1EB6	128.2
3	No Link	0	19	32768.0010B54C1EB6	128.3
4	No Link	0	19	32768.0010B54C1EB6	128.4
5	No Link	0	19	32768.0010B54C1EB6	128.5
6	No Link	0	19	32768.0010B54C1EB6	128.6
7	No Link	0	19	32768.0010B54C1EB6	128.7
8	No Link	0	19	32768.0010B54C1EB6	128.8
9	No Link	0	19	32768.0010B54C1EB6	128.9
10	No Link	0	19	32768.0010B54C1EB6	128.10
11	No Link	0	19	32768.0010B54C1EB6	128.11
12	No Link	0	19	32768.0010B54C1EB6	128.12

Parameter	Description
Port Status	Displays the current state of this port within the spanning tree: No Link No link has been established on this port. Disabled Port has been disabled by the user or has failed diagnostics. Blocked Port receives STA configuration messages, but does not forward packets. Listening Port will leave blocking state due to topology change, starts transmitting configuration messages, but does not yet forward packets. Learning Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. Forwarding The port forwards packets, and continues learning addresses. The rules defining port status are: - A port on a network segment with no other STA compliant bridging device is always forwarding. - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked. - All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
Forward Transitions	The number of times the port has changed status to forwarding state.
Designated Cost	The cost for a packet to travel from this port to the root in the current spanning tree configuration. The slower the media, the higher the cost.
Designated Bridge	The priority and MAC address of the device through which this port must communicate to reach the root of the spanning tree.
Designated Port	The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the spanning tree.

Spanning Tree Configuration

The following figures and tables describe Bridge STA configuration.

Switch

Usage	Enabled
Priority	32768

Parameter	Default	Description
Usage	Enabled	Enable this parameter to participate in an STA compliant network.
Priority	32,768	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. (Remember that the lower the numeric value, the higher the priority.) However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Range: 0 - 65535

When the Switch Becomes Root

Hello Time	2	seconds
Maximum Age	20	seconds
Forward Delay	15	seconds

Parameter	Default	Description
Hello Time	2	The time interval (in seconds) at which the root device transmits a configuration message. The minimum value is 1. The maximum value is the lower of 10 or $[(\text{Max. Message Age} / 2) - 1]$.
Max (Message) Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or $[2 \times (\text{Hello Time} + 1)]$. The maximum value is the lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$.
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. Maximum value is 30. Minimum value is the higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$.

STA Port Configuration

The following figure and table describe STA configuration for ports or modules.

Fast forwarding mode:

Port	Priority	Path Cost	Fast Forward
1	128	19	☒ Enable
2	128	19	☒ Enable
3	128	19	☒ Enable
4	128	19	☒ Enable
5	128	19	☒ Enable
6	128	19	☒ Enable
7	128	19	☒ Enable
8	128	19	☒ Enable
9	128	19	☒ Enable
10	128	19	☒ Enable
11	128	19	☒ Enable
12	128	19	☒ Enable

Parameter	Default	Description
Fast Forwarding Mode (All Ports)	Enabled	See "Fast Forward" in this table.
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
Path Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. The default and recommended range is: Standard Ethernet: 100 (50~600) Fast Ethernet: 19 (10~60) Gigabit Ethernet: 4 (3~10) The full range is 1 - 65535. Note: Path cost takes precedence over port priority.
Fast Forward	Enabled	This enables/disables Fast Forwarding for the selected port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding. Fast Forwarding enables end-node workstations and servers to overcome time-out problems when the Spanning Tree Algorithm is implemented in a network. Therefore, Fast Forwarding should only be enabled for ports that are connected to an end-node device.

Configuring Bridge MIB Extensions

The Bridge MIB includes extensions for managed devices that support Traffic Classes and Virtual LANs. To display and configure these extensions, use the Bridge Extension screen as shown below:

Bridge Capability

Extended Multicast Filtering Services	No
Traffic Classes	Yes
Static Entry Individual Port	Yes
VLAN Learning	SVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

Parameter	Description
Extended Multicast Filtering Services*	Enables filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
Traffic Classes	This switch provides mapping of user priorities to multiple traffic classes. (Refer to the Priority menu on page 3-22.)
Static Entry Individual Port	This switch enables static filtering for unicast and multicast addresses. (Refer to the Address Table Configuration on page 3-15.)
VLAN Learning	This switch uses Shared VLAN Learning (SVL), whereby each port maintains its own VLAN filtering database.
Configurable PVID Tagging	This switch allows you to override the default PVID (Port VLAN ID) assigned to untagged incoming frames under VLAN Port Configuration on page 3-30.
Local VLAN Capable*	A local bridge (that is, dedicated Spanning Tree) is applied to each individual VLAN.

* These functions are not available for the current firmware release.

Bridge Settings

Traffic Classes	☐ Enable
GMRP	☐ Enable
GVRP	☐ Enable

Parameter	Description
Traffic Classes*	Multiple traffic classes are supported by this switch as indicated under Bridge Capabilities. However, you can disable this function by clearing the check box for this parameter.
GMRP*	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. IGMP Snooping is currently used by this switch to provide automatic multicast filtering.
GVRP*	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLANs groups which extend beyond the local switch.

* These functions are not available for the current firmware release.

Priority

IEEE 802.1P defines up to 8 separate traffic classes. This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. You can use the Priority Menu to configure the default priority for each port, or to display the mapping for the traffic classes.

Port Priority Configuration

Inbound frames that do not have any VLAN tags are tagged with the input port's default VLAN ID (PVID) and the default ingress user priority as shown in the following screen, and then sorted into the appropriate priority queue at the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority queue of the output port. You can use the Port Priority Configuration screen to adjust default priority for any port as shown below.

Port	Default Ingress User Priority	Number of Egress Traffic Classes
1	0	2
2	0	2
3	0	2
4	0	2
5	0	2
6	0	2
7	0	2
8	0	2
9	0	2
10	0	2
11	0	2
12	0	2

Parameter	Description
Port	Numeric identifier for switch port.
Default Ingress User Priority	Default priority can be set to any value from 0~7, where 0~3 specifies the low priority queue and 4~7 specifies the high priority queue.
Number of Egress Traffic Classes	Indicates that this switch supports two priority output queues.

Port Traffic Class Information

This switch provides two priority levels with Weighted Fair Queuing for port egress. This means that any frames with a default or user priority from 0~3 are sent to the low priority queue “0” while those from 4~7 are sent to the high priority queue “1” as shown in the following screen.

Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7	Class Range
1	0	0	0	0	1	1	1	1	0-1
2	0	0	0	0	1	1	1	1	0-1
3	0	0	0	0	1	1	1	1	0-1
4	0	0	0	0	1	1	1	1	0-1
5	0	0	0	0	1	1	1	1	0-1
6	0	0	0	0	1	1	1	1	0-1
7	0	0	0	0	1	1	1	1	0-1
8	0	0	0	0	1	1	1	1	0-1
9	0	0	0	0	1	1	1	1	0-1
10	0	0	0	0	1	1	1	1	0-1
11	0	0	0	0	1	1	1	1	0-1
12	0	0	0	0	1	1	1	1	0-1

Parameter	Description
Port	Numeric identifier for switch port.
User Priority	Shows that user priorities 0~3 specify the low priority queue and 4~7 specify the high priority queue.
Class Range	The priority queue classes available on this switch.

Configuring Virtual LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 256 LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle a lot of NetBeui or IPX traffic. By using IEEE 802.1Q compliant VLANs, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, refer to "Virtual LANs" on page 4-2. The VLAN configuration screens are described in the following sections.

VLAN Basic Information

The VLAN Basic Information screen displays basic information on the VLAN type supported by this switch.

VLAN Version Number	1
Maximum VLAN ID	2048
Maximum Number of Supported VLANs	256
Current Number of 802.1Q VLANs Configured	1

Parameter	Description
VLAN Version Number	The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
MAX VLAN ID	Maximum VLAN ID recognized by this switch.
MAX Supported VLANs	Maximum number of VLANs that can be configured on this switch.
Current Number of VLANs Configured	The number of VLANs currently configured on this switch.

VLAN Current Table

This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports to the same untagged VLAN. The current configuration is shown in the following screen.

VLAN Entry Delete Count: 0

VLAN ID: 1

Up Time at Creation	0 d 0 h 0 min 0 s
Status	Permanent

Egress Ports

Unit 1, Port 1
Unit 1, Port 2
Unit 1, Port 3
Unit 1, Port 4
Unit 1, Port 5
Unit 1, Port 6
Unit 1, Port 7
Unit 1, Port 8

Untagged Ports

Unit 1, Port 1
Unit 1, Port 2
Unit 1, Port 3
Unit 1, Port 4
Unit 1, Port 5
Unit 1, Port 6
Unit 1, Port 7
Unit 1, Port 8

Parameter	Description
VLAN Entry Delete Count	The number of times a VLAN entry has been deleted from this table.
VLAN ID	The ID for the VLAN currently displayed.
Up Time at Creation	The value of System Up Time (sysUpTime) when this VLAN was created.
Status	Shows how this VLAN was added to the switch. Dynamic GVRP: Automatically learned via GVRP. Permanent: Added as a static entry.
Egress Ports	Shows the ports which have been added to the displayed VLAN group.
Untagged Ports	Shows the untagged VLAN port members.

VLAN Static List

Use this screen to create or remove VLAN groups.

Current:

1, , Enabled

<< Add

Remove

New:

VLAN ID (1-2048)	
VLAN Name	
Status	☐ Enable

Parameter	Description
Current	Lists all the current VLAN groups created for this system. Up to 256 VLAN groups can be defined. To allow this switch to participate in a VLAN group that extends beyond this switch, you must add the VLAN ID for the required external groups.
New	Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
Status	Enables/disables the specified VLAN.
Add	Adds a new VLAN group to the current list.
Remove	Removes a VLAN group from the current list. If a removed port is no longer be assigned to any other group as an untagged port, it will automatically be assigned to VLAN group 1 as untagged.

VLAN Static Table

Use this screen to modify the settings for an existing VLAN. You can add/delete port members for a VLAN from any unit in the stack. (Note that VLAN 1 is fixed as an untagged VLAN containing all ports in the stack, and cannot be modified via this screen.)

VLAN: 1

Name	
Status	☒ Enable

Parameter	Description
VLAN	The ID for the VLAN currently displayed. Range: 1-2048
Name	A user-specified symbolic name for this VLAN. String length: 8 alphanumeric characters
Status	Enables/disables the specified VLAN.

Use the following menu to add or remove a port to the displayed VLAN group. As you can see from this example, all ports are included in VLAN 1 by default.

Egress Ports

Members:

Unit 1, Port 1
Unit 1, Port 2
Unit 1, Port 3
Unit 1, Port 4
Unit 1, Port 5
Unit 1, Port 6
Unit 1, Port 7
Unit 1, Port 8

<< Add

Remove >>

Non-Members:

(none)

Parameter	Description
Egress Ports	Displays lists of the members and non-members of the specified VLAN.
Add	Adds the port selected in the non-members list to the VLAN members list.
Remove	Removes the port selected in VLAN members list and places it in the non-members list.

Note: If a removed port is no longer assigned to any other group as an untagged port, it will automatically be assigned to VLAN group 1 as untagged.

Use the menu shown below to prevent a port from being dynamically added to the displayed VLAN group through GVRP.

Forbidden Egress Ports

Members: (none)	<< Add Remove >>	Non-Members: Unit 1, Port 1 Unit 1, Port 2 Unit 1, Port 3 Unit 1, Port 4 Unit 1, Port 5 Unit 1, Port 6 Unit 1, Port 7 Unit 1, Port 8
--	---	--

Parameter	Description
Forbidden Egress Ports	Prevents a port from being automatically added to this VLAN via GVRP. Note that GVRP is not supported by the current firmware version.
Add	Adds the port selected in the non-members list to the members list.
Remove	Removes the port selected in the members list and places it in the non-members list.

Use the menu shown below to assign ports to the specified VLAN group as an IEEE 802.1Q tagged or untagged port. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged if they are connected to VLAN-unaware devices.

Untagged Ports

Members: Unit 1, Port 1 Unit 1, Port 2 Unit 1, Port 3 Unit 1, Port 4 Unit 1, Port 5 Unit 1, Port 6 Unit 1, Port 7 Unit 1, Port 8	<< Add Remove >>	Non-Members: (none)
--	---	--

Parameter	Description
Untagged Ports	Adds an authorized egress port to the displayed VLAN as an untagged port.
Add	Adds the port selected in the non-members list to the members list.
Remove	Removes the port selected in the members list and places it in the non-members list.

Note: If a removed port is no longer assigned to any other group as an untagged port, it will automatically be assigned to VLAN group 1 as untagged.

VLAN Static Membership by Port

Use the screen shown below to assign VLAN groups to the selected port. To perform detailed port configuration for a specific VLAN, use the VLAN Static Table (page 3-27).

Port Number:

Member:

1

Non-Member:

(none)

<< Add

Remove >>

Parameter	Description
Port Number	Port number on the switch selected from the upper display panel.
Add/Remove	Add or remove selected VLAN groups for the port indicated in the Port Number field.

VLAN Port Configuration

Use this screen to configure port-specific settings for IEEE 802.1Q VLAN features.

Port	PVID (1-2048)	Acceptable Frame Type	Ingress Filtering	GVRP Status	GVRP Failed Registrations	GVRP PDU Origin
1	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
2	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
3	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
4	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
5	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
6	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
7	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
8	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
9	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
10	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
11	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
12	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00

Parameter	Description
PVID	The VLAN ID assigned to untagged frames received on this port. Use the PVID to assign ports to the same untagged VLAN.
Acceptable Frame Type	This switch accepts "All" frame types, including VLAN tagged or VLAN untagged frames. Note that all VLAN untagged frames received on this port are assigned to the PVID for this port.
Ingress Filtering	If set to "True," incoming frames for VLANs which do not include this port in their member set will be discarded at the inbound port.
GVRP Status*	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. Note that GVRP must be enabled for the switch before this setting to take effect. (See "Configuring Bridge MIB Extensions" on page 3-20.)
GVRP Failed Registrations*	The total number of failed GVRP registrations, for any reason, on this port.
GVRP Last PDU Origin*	The Source MAC Address of the last GVRP message received on this port.

* GVRP is not available for the current firmware release.

IGMP Multicast Filtering

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The switch looks up the IP Multicast Group used for this service and adds any port that received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. (For more information, see "IGMP Protocol" on page 4-5.)

Configuring IGMP

This protocol allows a host to inform its local switch/router that it wants to receive transmissions addressed to a specific multicast address group. Use the IGMP Configuration screen to set key parameters for multicast filtering as shown below.

IGMP Status	☒ Enable
IGMP Query Count (2-10)	2
IGMP Report Delay (5-30)	10 seconds

Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
IGMP Query Count	The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports.
IGMP Report Delay	The time (in seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out that port and removes the entry from its list.

* This function is not available for the current firmware release.

Note: The default values are indicated in the sample screen.

IP Multicast Registration Table

Use the IP Multicast Registration Table to display all the multicast groups active on this switch, including multicast IP addresses and the corresponding VLAN ID.

VLAN ID:

Multicast IP Address:

Learned by: IGMP

Multicast Group Port List:

Unit 1, Port 7

Parameter	Description
VLAN ID	VLAN ID assigned to this multicast group.
Multicast IP Address	IP address for specific multicast services.
Learned by	Indicates the manner in which this address was learned: Dynamic or IGMP.
Multicast Group Port Lists	The switch ports registered for the indicated multicast service.

Port Menus

Port Information

The Port Information screen displays the port status, link state, the communication speed and duplex mode, as well as the flow control in use. To change any of the port settings, use the Port Configuration menu. The parameters are shown in the following figure and table.

Port	Admin Status	Link Status	Speed Status	Duplex Status	Flow Control Status
1	Enabled	Down	10M	Half	Disabled
2	Enabled	Down	10M	Half	Disabled
3	Enabled	Up	100M	Full	Disabled
4	Enabled	Down	10M	Half	Disabled
5	Enabled	Down	10M	Half	Disabled
6	Enabled	Down	10M	Half	Disabled
7	Enabled	Down	10M	Half	Disabled
8	Enabled	Down	10M	Half	Disabled
9	Enabled	Down	10M	Half	Disabled
10	Enabled	Down	10M	Half	Disabled
11	Enabled	Down	10M	Half	Disabled
12	Enabled	Down	10M	Half	Disabled

Parameter	Description
Admin Status	Shows if the port is enabled or not.
Link Status	Indicates if the port has a valid connection to an external device.
Speed Status	Shows the port speed (10M, 100M or 1000M).
Duplex Status	Displays the current duplex mode.
Flow Control Status	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.

Port Configuration

Use the Port Configuration menu to configure any port on the switch.

Flow control mode: Enable All Disable All

Port	Admin Status	Speed/Duplex Status	Flow Control Status
1	☒ Enable	Auto-Negotiation	Disabled
2	☒ Enable	Auto-Negotiation	Disabled
3	☒ Enable	Auto-Negotiation	Disabled
4	☒ Enable	Auto-Negotiation	Disabled
5	☒ Enable	Auto-Negotiation	Disabled
6	☒ Enable	Auto-Negotiation	Disabled
7	☒ Enable	Auto-Negotiation	Disabled
8	☒ Enable	Auto-Negotiation	Disabled
9	☒ Enable	Auto-Negotiation	Disabled
10	☒ Enable	Auto-Negotiation	Disabled
11	☒ Enable	Auto-Negotiation	Disabled
12	☒ Enable	Auto-Negotiation	Disabled

Parameter	Default	Description
Flow control mode (on all ports)	Disabled	See "Flow Control Status" in this table.
Admin Status	Enable	Allows you to disable a port due to abnormal behavior, and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Speed/Duplex Status	Auto-Negotiation	Used to set the current port speed, duplex mode, flow control, and auto-negotiation. Auto-negotiation is the default setting for 10BASE-T/100BASE-TX.
Flow Control Status	Disabled	Used to enable or disable flow control. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.

Expansion Port Information

The Expansion Port Information screen displays the port status, link state, the communication speed and duplex mode, as well as the flow control in use. To change any of the port settings, use the Expansion Port Configuration menu. The parameters shown in the following figure and table are for expansion ports.

Expansion Slot 1 - 2-Port 100Base-FX-SC(MMF)

Port	Admin Status	Link Status	Duplex Status	Flow Control Status
1	Enabled	Down	Half	Disabled
2	Enabled	Down	Half	Disabled

Expansion Slot 2 - Not Present

Port	Admin Status	Link Status	Duplex Status	Flow Control Status
------	--------------	-------------	---------------	---------------------

Parameter	Description
Admin Status	Shows if the port is enabled or not.
Link Status	Indicates if the port has a valid connection to an external device.
Duplex Status	Displays the current duplex mode.
Flow Control Status	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.

Expansion Port Configuration

Use the Expansion Port Configuration menus to configure any module port on the switch.

Expansion Slot 1 - 2-Port 100Base-FX-SC(MMF)

Port	Admin Status	Duplex Status	Flow Control Status
1	☒ Enable	Full ▼	Disabled ▼
2	☒ Enable	Full ▼	Disabled ▼

Expansion Slot 2 - Not Present

Port	Admin Status	Duplex Status	Flow Control Status
------	--------------	---------------	---------------------

Parameter	Default	Description																
Admin Status	Enable	Allows you to disable a port due to abnormal behavior, and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.																
Duplex Status	Auto-Negotiation	Used to set the current port speed, duplex mode, flow control, and autonegotiation. <table><tr><th>Port Type</th><th>Speed</th><th>Duplex Mode</th><th>Flow Control</th></tr><tr><td>100BASE-FX</td><td>100M</td><td>full duplex</td><td>auto</td></tr><tr><td>1000BASE-SX</td><td>1000M</td><td>auto</td><td>auto</td></tr><tr><td>1000BASE-LX</td><td>1000M</td><td>auto</td><td>auto</td></tr></table> The 1000BASE-SX and 1000BASE-LX ports are fixed at 1000 Mbps but autonegotiate duplex mode. The 100BASE-FX module is fixed at the indicated speed and duplex mode. All media types can autonegotiate flow control.	Port Type	Speed	Duplex Mode	Flow Control	100BASE-FX	100M	full duplex	auto	1000BASE-SX	1000M	auto	auto	1000BASE-LX	1000M	auto	auto
Port Type	Speed	Duplex Mode	Flow Control															
100BASE-FX	100M	full duplex	auto															
1000BASE-SX	1000M	auto	auto															
1000BASE-LX	1000M	auto	auto															
Flow Control Status	Disabled	Used to enable or disable flow control. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.																

Port Broadcast Storm Protect Configuration

Use the Port Broadcast Storm Protect Configuration screen to configure broadcast storm control for any port on the switch.

Broadcast Storm Protect mode: Enable All Disable All

Port	Protect Status	Threshold
1	☒ Enable	500
2	☒ Enable	500
3	☒ Enable	500
4	☒ Enable	500
5	☒ Enable	500
6	☒ Enable	500
7	☒ Enable	500
8	☒ Enable	500
9	☒ Enable	500
10	☒ Enable	500
11	☒ Enable	500
12	☒ Enable	500

Parameter	Default	Description
Broadcast Storm Protect Mode	Enabled	Allows you to enable/disable broadcast storm control for all ports on the switch.
Protect Status	Enabled	Enables/disables broadcast control for the port. When enabled, the switch will employ a broadcast-control mechanism if the packet-per-second threshold is exceeded. This mechanism limits the amount of broadcasts passed by the port to half of the received packet-per-second count. The control mechanism remains in effect until the number of received broadcasts falls back below the packet-per-second threshold.
Threshold	500	The packet-per-second threshold for broadcast packets on the port.

Port Security Configuration

Use the Port Security Configuration screen to enable and configure port security for the switch. Port Security allows you to configure each port with a list of MAC addresses of devices that are authorized to access the network through that port.

Port Number:

Status:

MAC Address List:

New Address:

Parameter	Description
Port Number	The port number on the unit.
Status	Port security can set to three states; Enabled, Disabled, or Learning. When set to Enabled, the switch will drop packets from the port if the source MAC address does not match one of the addresses in the MAC Address list. If set to Learning, the switch will add the source MAC address of all packets received on the port to the authorized MAC Address list.
MAC Address List	A list of the authorized MAC addresses that can access the network through the specified port.
New Address	A specific MAC address to be added to the list.
Add	Adds a new specified MAC address to the current list.
Remove	Removes a MAC address from the current list.
Clear All	Clears all the MAC addresses for the current port.

Using a Port Mirror for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a network sniffer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be included in the same VLAN as the source port. (See “VLAN Static List” on page 3-26.)

You can use the port mirror configuration screen to designate a single port pair for mirroring as shown below.

Status	☐ Enable
Mirror Source Unit	1
Mirror Source Port	1
Mirror Target Unit	1
Mirror Target Port	2

Parameter	Description
Status	Enables/disables port mirroring.
Mirror Source Unit	The switch containing the mirror source port.
Mirror Source Port	The port whose traffic will be monitored.
Mirror Target Unit	The switch containing the mirror target port.
Mirror Target Port	The port that will duplicate or “mirror” all the traffic happening on the monitored port.

Port Trunk Configuration

Port trunks can be used to increase the bandwidth of a network connection or to ensure fault recovery. You can configure up five trunk connections (combining 2~4 ports into a fat pipe) between any two standalone CheetahSwitch Workgroup-3726M switches, or up to 12 for an entire stack. However, before making any physical connections between devices, use the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, note that:

- The ports used in a trunk must all be of the same media type (RJ-45, 100 Mbps fiber, 1000BASE-SX or 1000BASE-LX). The ports that can be assigned to the same trunk have certain other restrictions as described on the following page.
- Ports can only be assigned to one trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including speed, duplex mode, and VLAN assignments.
- None of the ports in a trunk can be configured as a mirror source port or mirror target port.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.
- Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a loop.

Use the Port Trunking Configuration screen to set up port trunks as shown below:

Status List:

Trunk	Status
1	☒ Enable

Member List:

Current:

Trunk 1, Unit 1, Port 1
Trunk 1, Unit 1, Port 2

<<Add

Remove

New:

Trunk (1-12)	
Unit	1
Port	1

Parameter	Description
Trunk	A unique identifier for this trunk. You can configure up to five trunks per switch.
Status	Enables or disables the displayed trunk.
Member List	You can create up to 12 trunks for the entire stack by specifying the trunk identifier, switch unit and port number, and then clicking on the "Add" button. Each trunk can contain from 2 to 4 ports.

The RJ-45 ports used for one side of a trunk must all be on the same internal switch chip. The port groups permitted include:

Group 1

1, 2, 3, 4,
13, 14, 15, 16

Group 2

5, 6, 7, 8,
17, 18, 19, 20

Group 3

9, 10, 11, 12,
21, 22, 23, 24

The 100BASE-FX fiber ports used for one side of a trunk must all be on the same module. However, the 1000BASE-SX and 1000BASE-LX ports used for one side of a trunk may be on any switch in the stack, or both on the same switch if used standalone.

Media Module

100BASE-FX

Any ports on a single module.

1000BASE-SX

1000BASE-LX

Up to four Gigabit ports from any switch in the stack, or both Gigabit ports on two modules installed in a standalone switch.

For example, when using Gigabit ports to form a trunk within a stack, the Gigabit ports will all be at Port 25. In this case, you could specify a trunk group consisting of: (Unit1-Port25, Unit2-Port25, Unit3-Port25, Unit4-Port25), or two trunks consisting of: (Unit1-Port25, Unit2-Port25) and (Unit3-Port25, Unit4-Port25).

Port Statistics

Use the Port Statistics menu to display Etherlike or RMON statistics for any port on the switch. The statistics displayed are indicated in the following figure and table.

Etherlike Statistics

Etherlike Statistics display key statistics from the Ethernet-like MIB for each port. Error statistics on the traffic passing through each port are displayed. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). Values displayed have been accumulated since the last system reboot.

Port Number:

Etherlike Statistics:

FCS Errors	0	Late Collisions	0
Single Collision Frames	0	Excessive Collisions	0
Multiple Collision Frames	0	Internal MAC Transmit Errors	0
SQE Test Errors	0	Carrier Sense Errors	0
Deferred Transmissions	0	Frames Too Long	0
		Internal MAC Receive Errors	0

Parameter	Description
FCS Errors	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames*	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames*	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
SQE Test Errors*	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions*	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions*	The number of frames for which transmission failed due to excessive collisions.
Internal Mac Transmit Errors*	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carrier Sense Errors*	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frames Too Long	The number of frames received that exceed the maximum permitted frame size.
Internal Mac Receive Errors	The number of frames for which reception failed due to an internal MAC sublayer receive error.

* The reported values will always be zero because these statistics are not supported by the internal chip set used in this switch.

Note: Statistics are automatically refreshed every 60 seconds.

RMON Statistics

RMON Statistics display key statistics for each port or media module from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software.) The following screen displays overall statistics on traffic passing through each port. RMON statistics provide access to a broad range of statistics, including a total count of different frame types passing through each port. Values displayed have been accumulated since the last system reboot.

Drop Events	14361	Jabbers	0
Received Bytes	589428202	Collisions	0
Received Frames	967725	64 Bytes Frames	82498
Broadcast Frames	248101	65-127 Bytes Frames	119395
Multicast Frames	703686	128-255 Bytes Frames	139768
CRC/Alignment Errors	0	256-511 Bytes Frames	151144
Undersize Frames	0	512-1023 Bytes Frames	241621
Oversize Frames	0	1024-1518 Bytes Frames	233299
Fragments	0		

Parameter	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames	The total number of frames (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Parameter	Description
256-511 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Note: Statistics are automatically refreshed every 60 seconds.

Chapter 4: Advanced Topics

The CheetahSwitch Workgroup-3726M supports Layer 2 switching and other advanced features, which are described in this chapter.

Layer 2 Switching

When a frame enters a port, its destination MAC address is checked in the address database to see which port leads to this destination. If the destination address belongs to the incoming port, the frame is dropped or “filtered” because it is addressed to the local segment. If the destination address is found on another port, the frame is forwarded to that port and queued for output. But, if the destination address is not found in the address database, the frame is sent to one or more output ports based on the rules for handling tagged or untagged VLAN frames.

If the source MAC address of the frame was not found in the address database, it is recorded along with the incoming port number where it entered the switch. This information is then used to make later decisions for frame forwarding.

Switching involves the following steps:

- VLAN Classification
- Learning
- Filtering
- Forwarding
- Aging

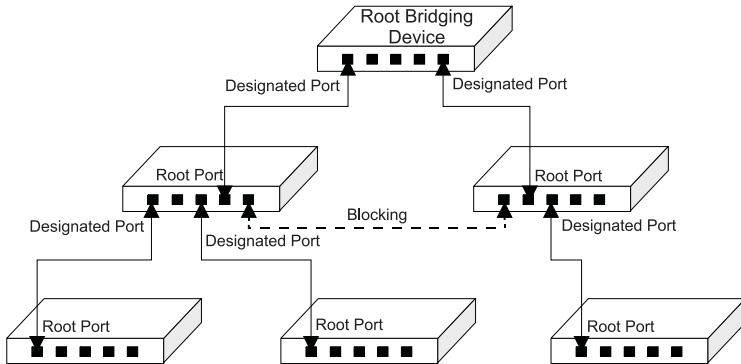
Spanning Tree Algorithm

The Spanning Tree Algorithm (that is, the STA configuration algorithm as outlined in IEEE 802.1D) can be used to detect and disable network loops, and to provide link backup. This allows the switch to interact with other bridging devices (including STA-compliant switches, bridges or routers) in your network to ensure that only one route exists between any two stations on the network. If redundant paths or loops are detected, one or more ports are put into a blocking state (stopped from forwarding packets) to eliminate the extra paths. Moreover, if one or more of the paths in a stable spanning tree topology fail, this algorithm will automatically change ports from blocking state to forwarding state to reestablish contact with all network stations.

The STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

The following figure gives an illustration of how the Spanning Tree Algorithm assigns bridging device ports.



Virtual LANs

Switches do not inherently support broadcast domains, which can lead to broadcast storms in large networks that handle a lot of IPX or NetBeui traffic. In conventional networks with routers, broadcast traffic is split up into physically separate domains to confine broadcast traffic to the originating group and provide a much cleaner network environment. This switch creates segregated broadcast domains based on easily configurable VLANs, these are then linked, as required, via a router or Layer 3 switch.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, but also allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security, since traffic must pass through a Layer 3 switch or a router to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 256 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging
- Port trunking with VLANs

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) it will participate in. (By default all ports are assigned to VLAN 1 as untagged ports.) Add a port as a tagged port (that is, a port attached to a VLAN-aware device) if you want it to carry traffic for one or more VLANs and the device at the other end of the link also supports VLANs. Then assign the port at the other end of the link to the same VLAN(s). However, if you want a port on this switch to participate in one or more VLANs, but the device at the other end of the link does not support VLANs, then you must add this port as an untagged port (that is, a port attached to a VLAN-unaware device).

Port-based VLANs are tied to specific ports. The switch's forwarding decision is based on the destination MAC address and its associated port. Therefore, to make valid forwarding and flooding decisions, the switch learns the relationship of the MAC address to its related port—and thus to the VLAN—at run-time. When the switch receives a frame, it assigns the frame to the port's default VLAN if the frame is untagged (determined by the PVID of the receiving port), or maps it for output to the broadcast domain associated with the frame's VLAN tag.

Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them using a router or Layer 3 switch.

Automatic VLAN Registration (GVRP)

GVRP defines a system whereby the switch can automatically learn the VLANs each endstation should be assigned to. If an endstation (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows

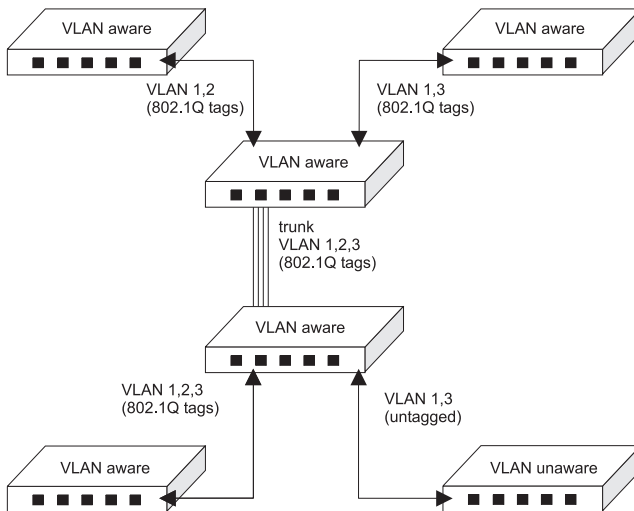
GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

Forwarding Traffic with Unknown VLAN Tags

This switch only supports 256 VLANs with VLAN IDs ranging from 1 to 2048, but the IEEE 802.1Q VLAN standard allows for VLAN IDs from 1 to 4094. Therefore, if this switch is attached to endstations that issue VLAN registration requests, it will have to forward unknown VLAN tags. This traffic can only be propagated to the rest of the network if automatic VLAN registration is enabled on your switch.

Forwarding Tagged/Untagged Frames

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. To forward a frame from a VLAN-aware device to a VLAN-unaware device, the switch first decides where to forward the frame, and then strips off the VLAN tag. However, to forward a frame from a VLAN-unaware device to a VLAN-aware device, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting this port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed (see page 2-44 or page 3-30).



Connecting VLAN Groups

The switch supports intra-VLAN communication using wire-speed switching. However, if you have devices in separate VLANs that must communicate, and it is not practical to include these devices in a common VLAN, then the VLANs can be connected via a Layer 3 switch or router.

Multicast Filtering

Multicasting sends data to a group of nodes instead of a single destination. The simplest way to implement multicasting is to broadcast data to all nodes on the network. However, such an approach wastes a lot of bandwidth if the target group is small compared to overall the broadcast domain.

Since applications such as video conferencing and data sharing are more widely used today, efficient multicasting has become vital. A common approach is to use a group registration protocol that lets nodes join or leave multicast groups. A switch or router can then easily determine which ports contain group members and send data out to those ports only. This procedure is called multicast filtering.

The purpose of multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches instead of flooding to all ports in the subnet (VLAN). This switch supports multicast filtering by passively monitoring IGMP Query and Report messages.

IGMP Snooping

A Layer 2 switch can passively snoop on IGMP Query and Report packets transferred between IP Multicast Routers/Switches and IP Multicast host groups to learn the IP Multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures multicast filters accordingly. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce the multicast traffic passing through your switch.

IGMP Protocol

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast router/switch. IGMP is a multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the responsibility of querying the LAN for group members.

Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast routers use this information, along with a multicast routing protocol such as DVMRP, to support IP multicasting across the Internet.

Note that IGMP neither alters nor routes any IP multicast packets. A multicast router/switch must be used to deliver IP multicast packets across different subnetworks.

Class-of-Service (CoS) Support

The CheetahSwitch Workgroup-3726M provides two transmit queues on each port, with a Weighted Fair Queuing scheme. This function can be used to provide independent priorities for various types of data such as real-time video or voice, and best-effort data.

Priority assignment to a packet in the CheetahSwitch Workgroup-3726M can be accomplished in any of the following ways:

- Priority can be explicitly assigned by end stations which have applications that require a higher priority than best-effort. This switch utilizes the IEEE 802.1P and 802.1Q tag structure to decide priority assignments for the received packets.
- A port may be manually configured as high priority. In this case, when any other port receives traffic from a high-priority port, that traffic is automatically placed in the high-priority output queue.

Port Trunks

Ports can be combined into an aggregate link to increase the bandwidth of a network connection or ensure fault recovery. You can group ports into trunks that consist of two, three or four ports, creating an aggregate bandwidth of up to 8 Gbps when grouping multiple Gigabit ports. Besides balancing the load across each port in the trunk, the additional ports provide redundancy by taking over the load if another port in the trunk should fail.

When using port trunks, remember that:

- Before removing a port trunk via the configuration menu, you must disable all the ports in the trunk or remove all the network cables. Otherwise, a loop may be created.
- To disable a single link within a port trunk, you should first remove the network cable, and then disable both ends of the link via the configuration menu. This allows the traffic passing across that link to be automatically distributed to the other links in the trunk, without losing any significant amount of traffic.

SNMP Management Software

SNMP (Simple Network Management Protocol) is a communication protocol designed specifically for managing devices or other elements on a network. Network equipment commonly managed with SNMP includes hubs, switches, bridges, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as monitor them to evaluate performance and detect potential problems.

Remote Monitoring

Remote Monitoring (RMON) provides a cost-effective way to monitor large networks by placing embedded or external probes on distributed network equipment (hubs, switches or routers). Network management software can access the probes embedded in network products to perform traffic analysis, troubleshoot network problems, evaluate historical trends, or implement proactive management policies. RMON has already become a valuable tool for network managers faced with a quickly changing network landscape that contains dozens or hundreds of separate segments. RMON is the only way to retain control of the network and analyze applications running at multi-megabit speeds. It provides the tools you need to implement either reactive or proactive policies that can keep your network running based on real-time access to key statistical information.

This switch provides support for basic RMON which contains the four key groups required for basic remote monitoring. These groups include:

Statistics: Includes all the tools needed to monitor your network for common errors and overall traffic rates. Information is provided on bandwidth utilization, peak utilization, packet types, errors and collisions, as well as the distribution of packet sizes.

History: Can be used to create a record of network utilization, packet types, errors and collisions. You need a historical record of activity to be able to track down intermittent problems. Historical data can also be used to establish normal baseline activity, which may reveal problems associated with high traffic levels, broadcast storms, or other unusual events. Historical information can also be used to predict network growth and plan for expansion before your network becomes too overloaded.

Alarms: Can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over the set interval). Alarms can be set to respond to either rising or falling thresholds.

Events: Defines the action to take when an alarm is triggered. The response to an alarm can include recording the alarm in the Log Table or sending a message to a trap manager. Note that the Alarm and Event Groups are used together to record important events or immediately respond to critical network problems.

Appendix A: Troubleshooting

Troubleshooting Chart

Troubleshooting Chart	
Symptom	Action
Cannot connect using Telnet, Web browser, or SNMP software	• Be sure to have configured the agent with a valid IP address, subnet mask and default gateway. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Check network cabling between the management station and the switch. • If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted. Try connecting again at a later time.
Can't access the on-board configuration program via a serial port connection	• Be sure to have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 19200 bps. • If the switch is configured for Auto (baud rate detection), the terminal emulator program must be set at 2400~19200 baud, 8 data bits, 1 stop bit, no parity, and flow control set to none. Also, you must first press the Enter key once to set the data rate and initialize the connection. • Check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B.
Forgot or lost the password	• Contact Accton Technical Support for help.

Upgrading Firmware via the Serial Port

You can upgrade system firmware by connecting your computer to the serial port on the switch, and using a console interface package that supports the XModem protocol. (See “Required Connections” on page 1-1.)

1. Restart the system by using the Restart System command or resetting the power by pulling out the power cord, waiting five seconds, and plugging it back in.
2. When the system initialization screen appears as shown below, press “D” to download system firmware, and then indicate the code type (1: Runtime, 2: POST, 3: Mainboard).

```
850 POST for L2, 06/07/2001

LOADER Version V1.02
POST   Version V1.11

----- Performing the Power-On Self Test (POST) -----
EPROM Checksum Test ..... PASS
Testing the System SDRAM ..... PASS
CPU Self Test ..... PASS
EEPROM Checksum Test ..... PASS
SEEPROM Checksum Test ..... PASS
MAC Address .....00-10-b5-fd-84-bb
----- Power-On Self Test Completed -----

(D)ownload System Image or (S)tart Application: [S]
```

For example, if you select 1 (for downloading agent firmware), the system will display the following message:

```
(D)ownload System Image or (S)tart Application: [S]

Select the Firmware Type to Download (1)Runtime (2)POST
(3)Mainboard [1]: 1
Your Selection: Runtime Code
Download code to FlashROM address 0x02880000
```

3. Change your baud rate to 115200 bps, and press Enter to enable download mode. From the terminal emulation program, select the file you want to download, set the protocol to XModem, and then initialize downloading.

- Notes:**
1. If you use Windows HyperTerminal, disconnect  and reconnect  to enable the new baud rate.
 2. The download file should be a CheetahSwitch Workgroup-3726M binary file from Accton; otherwise the agent will not accept it. The file naming convention is:
 Runtime program: Agent-Vx.yz,
 POST program: Boot-Vx.yx, and
 Mainboard program: 8051-Vx.yz

3. After the file has been downloaded, the console screen will display information similar to that shown below. Press “s” to start the management interface, change the baud rate back to 19200, and press Enter. The Logon screen will then appear.

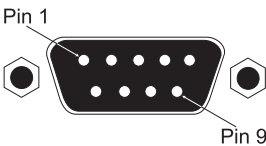
```
XModem Download to DRAM buffer area 0x00200000: ... SUCCESS !  
Verifying image in DRAM download buffer 0x00200000... SUCCESS !  
Update FlashROM Image at 0x02880000 ... SUCCESS !  
(D)ownload another Image or (S)tart Application: [S] s  
Change Baud Rate to 9600 and Press <ENTER>.
```

For details on managing the switch, refer to Chapter 2 for information on the out-of-band console interface, or Chapter 3 for information on the Web interface.

Appendix B: Pin Assignments

Console Port Pin Assignments

The DB-9 serial port on the switch's rear panel is used to connect to the switch for out-of-band console configuration. The on-board menu-driven configuration program can be accessed from a terminal, a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.



DB-9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #	PC DB25 DTE Pin #
BB	104	RxD (Received Data)	2	2	3
BA	103	TxD (Transmitted Data)	3	3	2
AB	102	SG (Signal Ground)	5	5	7

No other pins are used.

Console Port to 9-Pin DTE Port on PC

Switch's 9-Pin Serial Port	Null Modem	PC's 9-Pin DTE Port
2 RXD	<----- TXD ----->	3 TXD
3 TXD	----- RXD ----->	2 RXD
5 SGND	----- SGND -----	5 SGND

No other pins are used.

Console Port to 25-Pin DTE Port on PC

Switch's 9-Pin Serial Port	Null Modem	PC's 25-Pin DTE Port
2 RXD	<----- TXD ----->	2 TXD
3 TXD	----- RXD ----->	3 RXD
5 SGND	----- SGND -----	7 SGND

No other pins are used.

Glossary

Bandwidth Utilization

The percentage of packets received over time as compared to overall bandwidth.

BOOTP

Boot protocol used to load the operating system for devices connected to the network.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment such that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. (Formerly called Group Address Registration Protocol.)

Group Address Registration Protocol

See Generic Attribute Registration Protocol.

Internet Control Message Protocol (ICMP)

An integral part of the Internet Protocol (IP) that handles error and control messages. ICMP also includes an echo request/reply used to test whether a destination is reachable and responding.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging defines Ethernet frame tags which carry VLAN information. It allows switches to assign end-stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

In-Band Management

Management of the network from a station that is attached to the network.

Link Aggregation

See Port Trunk.

MIB

An acronym for Management Information Base. It is a set of database objects that contains information about the device. It defines variables needed by the SNMP protocol to monitor and control components in a network.

Out-of-Band Management

Management of the network from a station that is not attached to the network.

Port Mirroring

A method whereby data on a target port is mirrored to an analysis port for troubleshooting with a network sniffer or RMON probe. This allows data on the target port to be studied unobtrusively.

Port Trunk

Defines network link aggregation and trunking standards which specify how to create a single high-speed logical link that combines several lower-speed physical links.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific errors types.

Simple Network Management Protocol (SNMP)

An application protocol offering network management services in the Internet suite of protocols.

Serial Line Internet Protocol (SLIP)

A standard protocol for point-to-point connections using serial lines.

Spanning Tree Algorithm (STA)

A technology that checks your network for any loops. A loop can often occur in complicated network systems or systems with redundant links. Spanning-tree detects and directs data along the shortest path, maximizing the performance and efficiency of the network.

Spanning Tree Protocol (STP)

See Spanning Tree Algorithm.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Trivial File Transfer Protocol (TFTP)

The TCP/IP standard protocol for file transfer with minimal capability and minimal overhead. TFTP depends on the connectionless datagram delivery service, UDP.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, allowing users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Index

Numerics

- 802.1P port priority 3-22
- 802.1p port priority 4-6
- 802.1Q VLANs 2-40, 3-24, 4-2
- 802.3x flow control 2-22, 3-34, 3-36

A

- analyzer port configuration 2-30, 3-39
- automatic VLAN registration 4-3

B

- baud rate configuration 2-14, 3-5
- BOOTP
 - enabling 2-11, 3-10
 - for IP configuration 1-2
- Bridge Protocol Data Units (BPDUs) 4-2
- bridge STA information 2-28, 3-16
- Broadcast Storm Control 2-35, 2-45

C

- Class-of-Service 4-6
- community names, configuring 2-16, 3-11
- connections
 - serial port 1-1
 - Web browser 1-2
- console
 - interface
 - configuration buttons 2-3
- console interface
 - device control menu 2-21
 - logging off 2-53
 - login screen 2-1
 - main menu 2-4
 - management setup menu 2-9
 - network monitor menu 2-46
 - system information 2-6
 - system restart menu 2-53
- console port
 - configuration 2-14, 3-5
 - connections 1-1
 - pin assignments B-1

D

- downloading software 2-19, 3-13, A-2
- duplex mode configuration 2-22, 3-34, 3-36

E

- Etherlike statistics 3-42
- expansion port
 - configuration 3-36
 - information 3-35
- extended bridge configuration 2-36, 3-20

F

- Fast Forwarding 3-19
- Fast STA
 - See Fast Forwarding 3-19
- firmware
 - information 2-8, 3-8
 - upgrades 3-13, A-2
- flow control configuration 2-22, 3-34, 3-36

G

- GVRP 4-3

H

- hardware information 2-8, 3-8
- HTTP configuration 2-13

I

- IGMP 2-34
 - configuration 2-34, 3-31
 - protocol 4-5
 - query 4-5
 - report 4-5
 - snooping 4-5
- in-band connections 1-2
- Internet Group Management Protocol
 - See IGMP 4-5
- IP configuration 2-11, 3-10

L

- Layer 2 switching 4-1
- link aggregation 2-31, 3-40, 4-6
- login
 - configuration 2-18, 3-12
 - console interface 2-1

M

- MAC address of system 2-10
- MAC address table, displaying 2-50, 3-15
- management
 - options 1-1
 - software, SNMP 4-6

- mirror port configuration 2-30, 3-39
- multicast
 - filtering 4-5
 - configuring 2-34, 3-31
 - registration table, displaying 2-51, 3-32

O

- out-of-band connection 1-1

P

- password configuration 2-18, 3-12
- pin assignments, console port B-1
- Ping test 2-12
- port
 - configuration 2-22, 3-34, 3-37
 - information 2-23, 3-33
 - overlapping 4-3
 - priority 2-37, 3-22
 - STA Information 2-29, 3-17
 - trunks 4-6
 - configuration 3-40
- problems, troubleshooting A-1
- PVID 2-44, 3-20, 4-3

Q

- QoS configuration 2-37, 3-22

R

- remote monitoring (RMON) 4-7
- restarting the system 2-53
- restoring switch configuration 3-14

S

- security configuration 3-12
- serial port
 - configuration 2-14, 3-5
 - connections 1-1
 - XModem downloads A-2
- Simple Network Management Protocol
 - See SNMP 4-6
- SNMP 4-6
 - configuration 2-15, 3-11
 - management 1-2
- software downloads 2-19, 3-13, A-2
- Spanning Tree Algorithm
 - See STA 2-24
- STA 4-1
 - configuration 2-24, 3-16, 3-18

- statistics
 - port 2-47, 3-42
 - RMON 2-48, 3-43
- switch configuration 2-21
- switching
 - Layer 2 4-1
- system information 2-6, 3-7

T

- tagged
 - ports 4-3
 - VLANs 4-4
- TFTP downloads 2-19, 3-13
- time-out, console 2-14, 3-5
- traffic classes configuration 2-37, 3-22, 4-6
- trap managers, configuring 2-17, 3-12
- troubleshooting A-1
- trunk port configuration 2-31, 3-40

U

- unicast address table
 - configuring 2-52, 3-15
 - displaying 2-50, 3-15
- untagged
 - ports 4-3
 - VLANs 4-4
- upgrading software 2-19, 3-13, A-2
- upload, Web 3-13

V

- Virtual LANs
 - See VLANs 4-2
- VLANs 4-2
 - assigning ports 4-3
 - automatic registration 4-3
 - configuration
 - base information 2-40, 3-24
 - current table information 2-41, 3-25
 - port configuration 2-44, 3-30
 - static table configuration 2-42, 3-26
 - connecting 4-4
 - port overlapping 4-3
 - tagged 4-4
 - unknown tags 4-4
 - untagged 4-4

W

Web

- access requirements 3-1

- agent configuration 2-13

- browser connection 1-2

- interface

 - configuration buttons 3-3

 - home page 3-2

 - login 3-2

 - main menu 3-6

 - panel display 3-3

 - passwords 3-2

- upload 3-13

- Weighted Fair Queuing 2-37, 3-22

X

- XModem downloads A-2

AC-ES3726M
E022002-R01
F2.4761
150000017100A